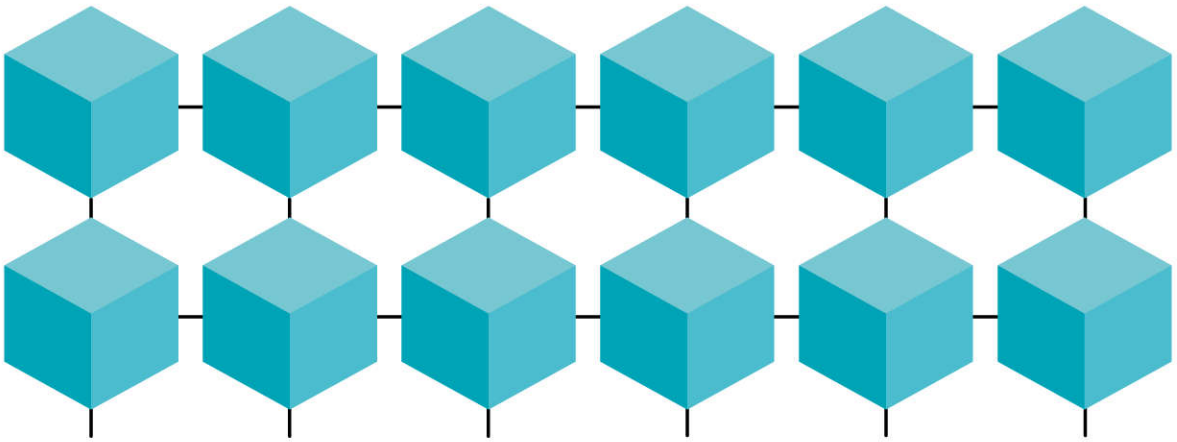
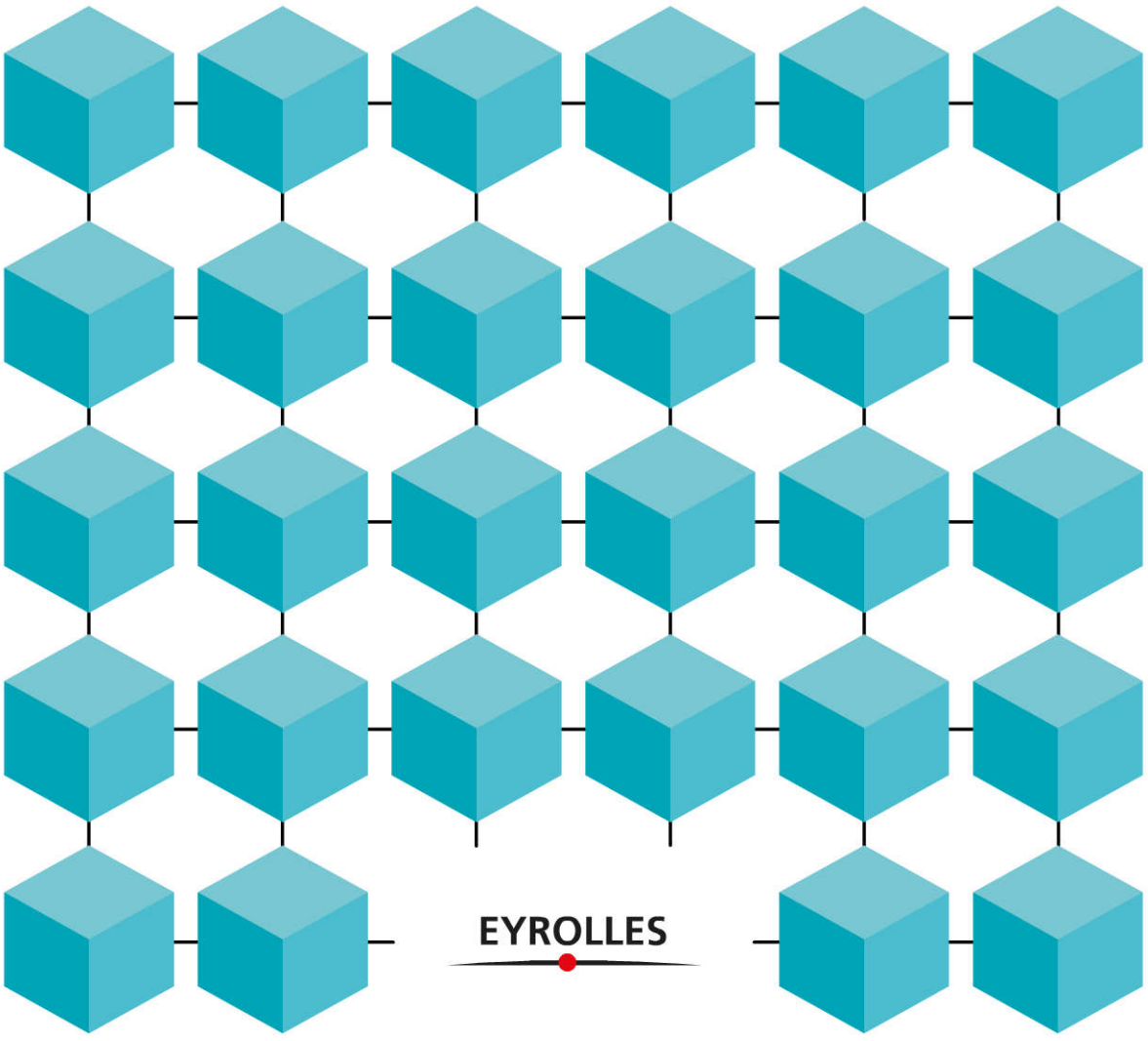


LAURENT LELOUP
Préface de William Mougayar

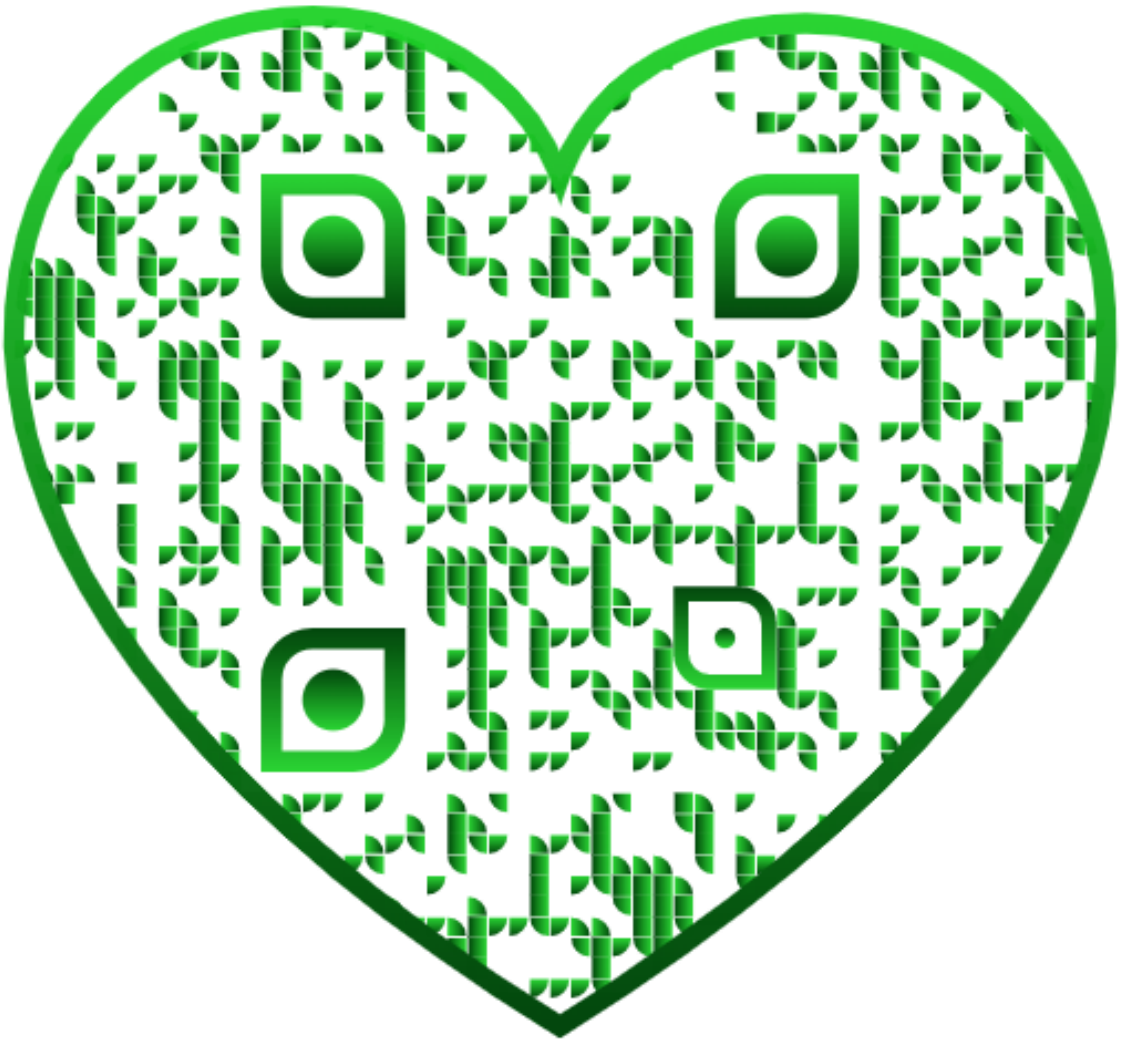
BLOCKCHAIN

La révolution de la confiance

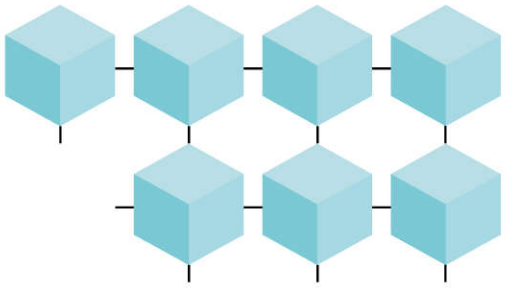


EYROLLES

Copyright © 2017 Eyrolles.



LA TECHNOLOGIE QUI POURRAIT « UBÉRISER UBER »



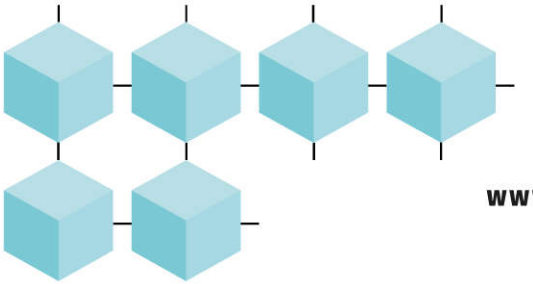
« Deuxième révolution numérique », « ubérisation ultime », « machine à confiance »... la blockchain laisse présager une révolution des usages comparable à celle portée par l'Internet dans les années 90.

La promesse de la blockchain est en effet majeure : des transactions instantanées à des coûts minimes et sans organe central de contrôle. Cette technologie a le potentiel de totalement changer les règles du jeu dans de nombreux secteurs économiques, à commencer par le système bancaire.

Comment se préparer ? Laurent Leloup décrypte de façon très pédagogique le fonctionnement d'une blockchain, les expériences en cours, les perspectives. Surtout, il pointe les questions à se poser et aide à diagnostiquer les opportunités liées à la blockchain dans chaque secteur.

Au-delà des implications économiques, c'est une profonde transformation sociétale qui s'annonce. Car la blockchain est avant tout une révolution de la confiance, portée non plus par un tiers de confiance – banquier, notaire, etc. –, mais par un système décentralisé et partagé. Un nouveau monde se profile.

Laurent Leloup *a fondé en 2006 Finyear Group, qui publie les quotidiens* Finyear & Blockchain Daily News *et produit de nombreux événements. En 2016, il a cofondé Blockness, une startup centrée blockchain, France Blocktech, l'association de l'écosystème blockchain français, et Blockchain Valley (campus, centre de formation, incubateur).*



www.editions-eyrolles.com

Copyright © 2017 Eyrolles.

Blockchain

Copyright © 2017 Eyrolles.

Groupe Eyrolles
61, bd Saint-Germain
75240 Paris Cedex 05
www.editions-eyrolles.com

Illustrations : Pierre Leloup

Copyright © 2017 Eyrolles.

En application de la loi du 11 mars 1957, il est interdit de reproduire intégralement ou partiellement le présent ouvrage, sur quelque support que ce soit, sans autorisation de l'éditeur ou du Centre français d'exploitation du droit de copie, 20, rue des Grands-Augustins, 75006 Paris.

© Groupe Eyrolles, 2017
ISBN : 978-2-212-56665-9

Laurent Leloup

Blockchain

La révolution de la confiance

Copyright © 2017 Eyrolles.

EYROLLES

Copyright © 2017 Eyrolles.

Sommaire

Préface 3

Introduction 7

Chapitre 1
La blockchain, c'est quoi ?

Démystifier la blockchain 13
Définition 13
Les grands principes de la blockchain 14
D'Internet à la blockchain 16
Comment ça fonctionne ? 17
À quoi ça sert ? 20
Le secteur de la banque, premier secteur affecté 20
Quelques champs d'application 24

Chapitre 2
La blockchain aujourd'hui

La blockchain Bitcoin 29
Un peu d'histoire 29
Définition 33
Fonctionnement 34
Évolution, scalabilité 55
Blockchain Ethereum 73
Un peu d'histoire 73
Chronologie des versions 75
Définition 76
Fonctionnement 78
Smart contracts, DAO 79
Protocoles de consensus distribués 91
Définition 91

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Les types de blockchain 93
Consensus 97
Écosystème 103
Pour résumer 116

Chapitre 3
La blockchain en pratique

Cas d'usage, applications 121
Principes de la technologie blockchain 121
Diverses applications 129
Blockchain et entreprises, une opportunité à saisir 158
La blockchain, une technologie disruptive bénéfique pour les entreprises 159
Qu'est-ce qu'un bon cas d'usage « blockchain de consortium » ? 161
Quelle technologie adopter ? 166
Gouvernance et droit 169
Qu'est-ce qu'un logiciel libre ? 170
Qui est propriétaire de la blockchain ? 171
La force juridique des opérations réalisées dans la blockchain 172
Pourquoi un smart contract n'est pas un contrat 174

Chapitre 4
La blockchain demain

Révolution en marche 179
Les révolutions industrielles 179
De la révolution informatique au Web 2.0 182
Pensées et visions 188
L'économiste américain qui voulait remplacer le cash par le bitcoin 189
Blockchain, révolution sociétale et économique ? 191
La blockchain comme révolution… mais révolution de quoi ? 195

Conclusion 201
Remerciements 205
Ressources 211
Index 219

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

À mon épouse Marie,

et à mes fils Yohan et Pierre

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Copyright © 2017 Eyrolles.

Préface

La blockchain est le meilleur nouvel outil de cette décennie. Pourtant, en ce début 2017, ce sujet connaît toujours un grave déficit de compréhension et de sensibilisation de la part du grand public. C'est un point de départ problématique pour la pleine réussite de son évolution.

Voici pourquoi le travail de Laurent Leloup dans ce livre est si important, car il nous aide à comprendre la blockchain, ainsi que ses multiples caractéristiques.

Bien que ce livre vous soit d'une grande aide pour comprendre la blockchain, cela n'est pas suffisant, car vous devez également vous entraîner à « comment penser blockchain ». Votre devoir, pour vraiment vous lancer dans un projet blockchain, sera de faire preuve de curiosité sur le sujet car tout n'est pas évident à comprendre de prime abord.

Dire que la blockchain est polyvalente est un euphémisme. Selon qui vous êtes et ce que vous faites, la blockchain aura quelque chose de différent à vous offrir. Ainsi, pour un développeur, la blockchain sera l'environnement de développement le plus excitant depuis l'avènement du langage Java en 1995, tandis que, pour une entreprise, la blockchain sera un puissant catalyseur pour la réingénierie des opérations commerciales et des relations externes, alors que pour un entrepreneur, la blockchain permettra de disrupter et d'inventer de nouveaux modèles sans crainte de se lancer avec simplement un petit nombre de clients.

La blockchain n'est pas un seul et même objet, un produit unique, une simple tendance ou une fonctionnalité particulière. La blockchain est composée de multiples pièces dont

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

certaines d'entre elles travaillent ensemble, et d'autres d'une façon autonome et indépendante. En raison de ces caractéristiques modulaires, la blockchain offre un éventail infini de choix d'applications.

L'évolution de la blockchain véhicule beaucoup d'ambition. Bien que la théorie de la blockchain soit bien systématique, comme vous le découvrirez dans ce livre, plus vous pourrez combler les écarts entre la théorie et la pratique avec des cas réels (*a priori* les vôtres ?) et plus vous diminuerez le nombre d'obstacles sur le chemin qui vous conduit vers la réussite du déploiement de vos propres cas d'usage.

Le message de la blockchain est simple, mais fort : il s'agit avant tout d'innover. Il ne s'agit pas seulement de découvrir un meilleur Web, d'inventer une meilleure banque ou de fournir un meilleur service. La survie de la blockchain dépendra de ce que vous en ferez, et cela ne reposera pas seulement sur ses caractéristiques techniques. Son adoption sera progressive, à commencer par les développeurs et les start-upers, puis par les gens du techno-business, suivis par les entreprises qui découvriront le potentiel du changement, puis du grand public qui exigera les changements, et enfin des organisations qui avaient jusqu'alors résisté au changement.

Mais pour y arriver, nous aurons besoin de plus d'utilisateurs d'applications blockchain, de plus d'applications à créer, et de beaucoup plus de développeurs. À long terme, la plupart des utilisateurs ne sauront pas ou ne réaliseront pas qu'il y a une blockchain dans le logiciel ou le service avec lequel ils interagissent. Tout comme aujourd'hui, nous recherchons et évaluons les capacités d'une application en fonction de ses vertus, non pas parce qu'elle est une application mobile, ni parce qu'elle fonctionne sur une base de données, ni parce qu'elle est basée sur une technologie quelconque.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Au même titre que l'économie du Web, la blockchain créera une nouvelle économie, et nous ne devons pas perdre de vue ce potentiel. L'économie crypto-tech sera une économie fondée sur la confiance décentralisée (à la naissance), tant sur le plan politique que sur le plan architectural. La blockchain donnera un accès égal à tout le monde et réduira le niveau des obstacles à tous ses participants.

Alors que la diffusion et le partage de l'information étaient le créneau que le Web avait initialement abordé, la fonction de base de la blockchain est la transmission des valeurs. Voilà l'ampleur de la compréhension fondamentale que vous devez assimiler sur la blockchain – et presque tout ce qui suit émane de cette idée fondatrice.

En dépit de tout l'émoi qu'elle a engendré, nous devons garder à l'esprit que la blockchain est essentiellement une promesse de la technologie. Comme toute promesse, il faut du temps pour qu'elle se réalise. Mais pour remplir toutes ces promesses, nous aurons besoin de millions de développeurs compétents en technologie blockchain, de millions de business leaders, et de millions d'utilisateurs passionnés et engagés.

Tandis que l'avenir de la blockchain peut être vu à travers l'histoire du Web, ne regardons pas en arrière, hâtons-nous d'aller de l'avant.

Un grand merci à Laurent pour avoir repoussé les limites de notre compréhension de la blockchain, car la pédagogie est une tâche difficile mais aussi un noble défi à relever.

William Mougayar[1]

1. Auteur de *The Business Blockchain*, Wiley, 2016.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Copyright © 2017 Eyrolles.

Introduction

Lorsque *The Economist* titrait en octobre 2015 : « Blockchain, the Trust Machine », le web et les réseaux sociaux ont très rapidement et massivement relayé l'article.

Pensez-donc, nous sommes fin 2015, le mot « blockchain » n'a pas encore atteint le pic de notoriété qu'il connaît aujourd'hui et le magazine *The Economist*, donc pas n'importe lequel, titrait en couverture que la blockchain était une machine à créer de la confiance et que la technologie derrière le bitcoin pourrait transformer la façon dont fonctionne l'économie, rien que ça.

En fait, de quoi réveiller n'importe quelle rédaction… Ce qui n'a pas traîné car, dans les heures puis les jours qui ont suivi, l'ensemble des blogs, quotidiens, magazines et autres médias relayaient « l'article choc », avec plus ou moins de vérités sur la techno blockchain, le bitcoin et autres crypto-machins. Mais bon, la dynamique était enclenchée et la bombe médiatique de *The Economist* avait fait son effet.

Depuis octobre 2015 la pression médiatique n'est quasiment pas retombée et le nombre d'articles produits par jour sur la techno blockchain, les monnaies numériques et autres *distributed ledgers* est tout simplement phénoménal…

Cette annonce aura eu au moins une vertu : celle de parler de la blockchain, du bitcoin, des crypto-monnaies et des protocoles de consensus distribués, et d'initier la formation du public à une technologie disruptive, qualifiée de « révolutionnaire » par Don Tapscott et en voie d'ubériser Uber, « l'ubérisation ultime », comme le déclarait Philippe Herlin lors d'une interview.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Un peu plus d'un an est passé et peu de projets ont vu le jour : beaucoup d'annonces mais peu de réalisations concrètes, hormis quelques prototypes en cours de développement. Mais, me direz-vous, n'est-ce pas le lot d'une technologie naissante ?

Par contre, ce qu'il faut retenir de tout cet emballement médiatique et des échanges multiples et variés qui s'en sont suivis, c'est que l'innovation de la blockchain, dixit Ludwig Siegele, l'auteur de l'article publié dans *The Economist*, ce n'est pas l'argent… mais la confiance.

Rendez-vous compte, une technologie révolutionnaire, qui va disrupter de nombreux modèles d'affaires, complètement transformer l'économie et la société, et qui apporte quoi comme innovation ? La confiance.

Nous voici maintenant au milieu du gué, la pression médiatique va baisser en régime, les consultants vont monter en compétence, les entreprises, grandes puis moyennes, vont s'approprier la technologie, les projets vont se multiplier, les cas d'usage également, la technologie va progresser, les investisseurs vont se réveiller et au bout du bout nous aurons une seule vision novatrice, celle de la confiance partagée. C'est cela la promesse de la blockchain.

Il ne faut pas chercher à comprendre si l'on va être disrupté, transformé, ubérisé, il faut chercher dans son propre *business model*, dans ses relations avec ses clients, ses fournisseurs, ses personnels, où et comment nous pouvons apporter de la confiance.

Après l'avènement d'Internet des années 1990 puis de la blockchain Bitcoin (et son bitcoin) de Satoshi Nakamoto, les générations X et Y nous ont récemment montré la voie de plus de partage et de transparence avec l'avènement des réseaux sociaux.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Le pari perdu d'Internet de placer l'humain au cœur de sa technologie pour plus de pouvoir et de liberté sera peut-être relevé par la technologie blockchain.

Aujourd'hui nous avons une technologie « trustnomics[1] » qui peut insuffler de la confiance dans l'économie, la démocratie, la société… Alors saisissons cette opportunité, relevons le défi et lançons les machines à créer de la confiance dans les organisations et entre les individus.
2017 sera l'année de la naissance de la confiance partagée.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

1. http://www.trustnomics.net

Copyright © 2017 Eyrolles.

Chapitre 1

La blockchain, c'est quoi ?

« Qui manque de connaissance
est sans cesse à la merci du changement. »
Rémi Belleau

Copyright © 2017 Eyrolles.

Copyright © 2017 Eyrolles.

Démystifier la blockchain

Définition

Définir la blockchain en quelques mots n'est pas chose aisée car selon son mode de pensée, ses acquis, ses expériences, chaque lecteur ne sera pas réceptif de la même façon à une définition ou à une autre.

Voici plusieurs définitions qui, *crescendo*, devraient vous permettre de mieux comprendre ce qu'est la blockchain :

- Simpliste : une blockchain est un grand livre de compte ouvert et accessible à tous en écriture et en lecture et qui est partagé sur un grand nombre d'ordinateurs à travers le monde.
- Basique : une blockchain est un logiciel qui stocke et transfère de la valeur ou des données *via* Internet, de façon transparente et sécurisée, et sans organe central de contrôle.
- Littérale : une blockchain désigne une chaîne de blocs (conteneurs numériques) dans lesquels sont stockées des informations de toute nature : transactions, contrats, titres de propriétés, œuvres d'art, etc.
- Généraliste : une blockchain est une technologie pour une nouvelle génération d'applications transactionnelles qui, grâce à un mécanisme de consensus collectif couplé avec l'utilisation d'un grand livre de compte public, décentralisé et partagé, établit la confiance, la responsabilité et la transparence tout en rationalisant les processus d'affaires.
- Technique : une blockchain est une nouvelle technologie de base de données s'appuyant et tirant pleinement profit d'Internet, du protocole libre, de la puissance de calcul et de la cryptographie. Cette base de données transactionnelle distribuée est comparable à un grand livre comptable

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

(registre ou *ledger*) dans lequel chaque nouvelle transaction est écrite à la suite des autres, sans avoir la possibilité de modifier ou d'effacer les précédentes. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (consensus) entre les membres ou participants (nœuds).

On peut aussi proposer cette définition, qui résume l'ensemble des précédentes : une blockchain est une base de données transactionnelle distribuée, comparable à un grand livre comptable décentralisé et partagé, qui stocke et transfère de la valeur ou des données *via* Internet, de façon transparente, sécurisée, et autonome car sans organe central de contrôle. Ce registre est actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie (consensus) entre les membres ou participants (nœuds). Chaque membre du réseau possède une copie à jour du grand livre (en temps quasi réel) et le contenu est toujours en phase avec l'ensemble des participants.

Ainsi, la blockchain :

- permet l'automatisation de la transaction en supprimant les tiers ;
- est un système de consensus distribué et de confiance partagée ;
- est une infrastructure de certification et de notarisation.

Les grands principes de la blockchain

Les principes sur lesquels est fondée la blockchain sont les suivants :

- le *grand livre distribué* ou *distributed ledger* ou registre 2.0 construit sur le modèle des livres comptables et partagé entre les participants ;

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

- la *décentralisation* et la *désintermédiation* : aucune autorité centrale ne contrôle la blockchain, il n'y a pas de tiers de confiance ;
- le *consensus* : le fait qu'une transaction soit acceptée ou rejetée est le fruit d'un consensus distribué et non d'une institution centralisée (différentes formes de consensus existent) ;
- l'*immutabilité* : il est impossible de modifier ou de supprimer des écritures ;
- la *confiance partagée* et la *transparence* : il y a partage des données, des opérations et du consensus.

En résumé, passer par un mécanisme de consensus collectif plus utiliser un grand livre ouvert, décentralisé et partagé entraîne la *confiance*, la *transparence* et le *partage*.

La blockchain ne se limite pas à la blockchain Bitcoin ou à la blockchain Ethereum[1]. En effet, ce n'est pas une blockchain, mais plusieurs types de blockchains qui existent, cohabitent, voire interagissent. Ainsi, une blockchain peut posséder des spécificités techniques pour des utilisations ou des applications particulières.

La technologie blockchain change les règles du jeu : moins de centralisation, moins d'autorité, plus de partage. Ainsi, la blockchain apporte une infrastructure de confiance algorithmique distribuée ou *consensus-as-a-service* (consensus à la demande).

C'est en abordant ces aspects « d'infrastructure » que de nombreux observateurs ont tenté de rapprocher la technologie blockchain avec Internet, voire ont considéré qu'elle dépasserait Internet.

1. Bitcoin et Ethereum : voir le chapitre suivant.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

D'Internet à la blockchain

Afin d'illustrer ces propos nous vous livrons ce petit comparatif :

- Internet a permis l'automatisation de la relation (et de la mise en relation) *versus* la blockchain permet l'automatisation de la transaction en supprimant les tiers de confiance ;
- Internet est un système de publication décentralisé *versus* la blockchain est un système de consensus distribué ;
- Internet est une infrastructure de publication *versus* la blockchain est une infrastructure de certification.

Nous pourrions résumer[1] la période 1994-2015 (année zéro de la blockchain) par l'évolution suivante :

- 1994 : Internet :
  - communications personnelles ;
  - auto- publication ;
  - e-commerce ;
  - réseaux sociaux.
- 2015 : promesse de la blockchain :
  - décentralisation de la confiance ;
  - flux de valeur sans intermédiaire.

Il n'y a donc pas d'opposition entre blockchain et Internet mais une évolution technologique (voire une révolution [voir le chapitre 4]) qui vient compléter, voire disrupter, de très nombreux usages que nous aborderons dans les pages suivantes.

1. Petit résumé basé sur une illustration du livre *The Business Blockchain* (http://thebusinessblockchain.com/) de William Mougayar (http://www.slideshare.net/OuiShare/william-mougayar-the-promise-of-a-centerless-world).

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Comment ça fonctionne ?

Pour fabriquer et faire fonctionner une blockchain, il faut un registre (la chaîne de blocs, par exemple, pour Bitcoin), une cryptographie avec des clés pour sécuriser les échanges, un algorithme (consensus) pour valider les transactions et un réseau pair à pair[1] pour que le tout fonctionne. Vous y ajoutez des participants et voilà brièvement résumés les ingrédients dont vous aurez besoin.

Prenons l'exemple de la blockchain Bitcoin, dont nous explorerons la genèse, le fonctionnement et les principes dans le chapitre suivant, et décrivons son fonctionnement général en quatre étapes :

- Étape n° 1 : deux parties s'accordent sur les termes d'une transaction (transfert d'argent, actifs, titres financiers, etc.).
- Étape n° 2 : le registre est « scanné » par les membres du réseau. Par l'analyse de son historique, les membres du réseau s'assurent que le vendeur possède effectivement l'actif ou les fonds qu'il vend.
- Étape n° 3 : si tel est le cas, la transaction est validée et ajoutée au dernier bloc de la chaîne.
- Étape n° 4 : le registre est diffusé à l'ensemble du réseau. Son caractère distribué assure sa protection. Pour falsifier les transactions, il faudrait modifier les registres de l'intégralité des membres (nœuds) du réseau.

1. Lire cet article très instructif sur le sujet : https://interstices.info/jcms/c_8622/les-reseaux-de-pair-a-pair

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

L'analyse de David Daoud

« La blockchain Bitcoin a été la première à être définie comme une chaîne de blocs dans laquelle chaque transaction est cryptée pour devenir un bloc. La transaction suivante est à son tour cryptée sur la base du bloc précédent et ainsi de suite, d'où la notion de chaîne de blocs ou *block chain* devenue Blockchain (en un seul mot)[1]. »

En revanche, pour être valide, chaque transaction doit être signée, au sens cryptographique du terme, en utilisant de la cryptographie asymétrique[2] (clé privée/clé publique).

Par conséquent, trois informations sont nécessaires pour effectuer une transaction sur une blockchain de type Bitcoin :

- la clé privée de l'adresse débitée ;
- la clé publique de l'adresse créditée ;
- le montant de la transaction.

Une adresse bitcoin est représentée au format ASCII[3] grâce à un codage dédié sur 58 caractères alphanumériques : les chiffres et les lettres majuscules et minuscules, à l'exception des lettres et chiffres l, I, 0 et O, que Satoshi Nakamoto[4] a exclus car ces caractères se ressemblent dans certaines fontes. La première adresse créée était : 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa44.

1. Citation de David Daoud (Maltem Consulting) : http://www.finyear.com/Les-grands-principes-de-la-blockchain-et-son-impact-dans-l-industrie-financiere_a36219.html
2. http://www.blockchaindailynews.com/glossary/
3. ASCII (American Standard Code for Information Interchange) ou Code américain normalisé pour l'échange d'information. C'est une norme de codage de caractères en informatique ancienne et connue pour son influence incontournable sur les codages de caractères qui lui ont succédé.
4. Satoshi Nakamoto est l'inventeur du Bitcoin. Pour plus de détails, rendez-vous au chapitre suivant aux paragraphes consacrés à « La blockchain Bitcoin ».

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

(Par exemple, mon adresse bitcoin est :
112BekzNCw8xEfwtpwDgKr3zEfUgyuxUZV.)

Une adresse bitcoin est la seule information nécessaire pour recevoir des bitcoins. Il n'est pas nécessaire d'exécuter le logiciel Bitcoin pour la réception, il suffit de communiquer une adresse et seul le payeur se charge d'envoyer la transaction complète au reste du réseau.

Le grand public découvre peu à peu le bitcoin, les monnaies numériques et enfin la blockchain, mais sans trop comprendre ce qu'elle représente et à quoi elle sert. Il est vrai que le brouhaha médiatique autour de ses usages et le manque de vulgarisation de cette nouvelle technologie n'aident pas à la compréhension.

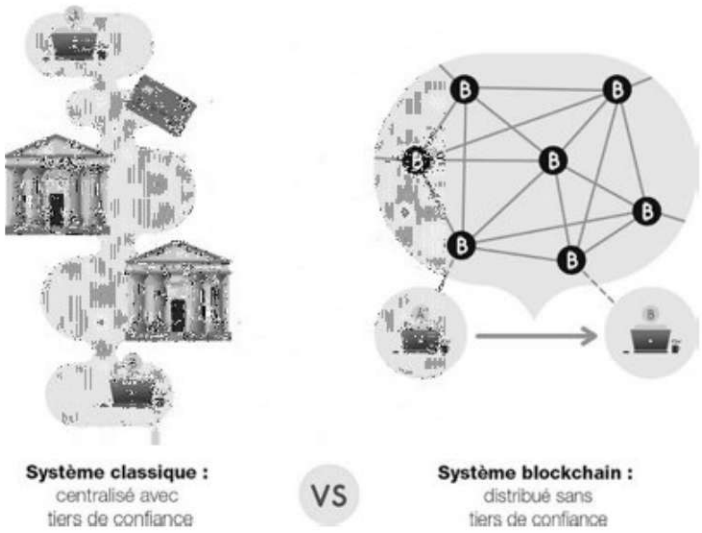
Ainsi, notre époque serait comparable à celle de la naissance d'Internet où le grand public entendait parler d'une technologie révolutionnaire sans en comprendre forcément le fonctionnement mais en saisissant bien les impacts sur l'économie et la société.

« La blockchain est comme Internet avant l'arrivée du navigateur[1] » : aujourd'hui, lorsque nous naviguons sur des sites ou réalisons des transactions *via* un PC ou un smartphone, il ne nous est pas utile de comprendre ce qu'est Internet et comment il fonctionne. Il en sera de même pour la blockchain lorsque les premiers cas d'usage arriveront et que les interfaces auront été développées.

1. Citation de Chris Skinner dans http://thefinanser.com/2016/07/blockchain-like-internet-browser.html/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles



À QUOI ÇA SERT ?

Le secteur de la banque, premier secteur affecté

La blockchain, solution inédite, décentralisée, sécurisée et transparente, permet de stocker, d'échanger, d'authentifier et de vérifier des informations pour un coût faible et supporté par l'utilisateur, donc sans tiers de confiance. C'est aussi sur ce point d'absence de tiers de confiance que se situent la principale innovation et l'originalité de la technologie blockchain.

L'application la plus connue de la technologie blockchain est la crypto-monnaie, ou crypto-devise ou encore monnaie numérique, comme le bitcoin, mais la technologie peut aussi être utilisée dans de nombreux autres domaines.

Pour l'instant, nous n'apercevons que quelques cas d'usage, mais les possibilités semblent être extrêmement nombreuses et dans tous les domaines de l'économie et de la société. Et ces possibilités se multiplient avec les nouvelles technologies blockchain émergentes.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Lors de la création de la blockchain Bitcoin (2009), le but de son inventeur n'était pas de servir le monde de la finance, mais bien au contraire de s'y substituer. Les banques ont commencé à découvrir au fil des années que cette technologie risquait de fortement disrupter leur modèle d'affaires et représentait à la fois une menace et une opportunité.

Philippe Herlin[1], lors d'une interview accordée au journal *Le Monde* en octobre 2015 et dans laquelle étaient évoquées les applications possibles de la technologie blockchain dans le secteur bancaire et financier, déclarait : « La blockchain, c'est l'ubérisation ultime. Même les services uberisés sur Internet peuvent l'être encore : Uber, Airbnb… ils paient des ingénieurs, des informaticiens[2]. »

En France, à partir du mois d'octobre 2015, les médias se firent l'écho d'une révolution[3] à venir, d'une technologie qui allait réécrire le business, la finance et même la société. Le battage médiatique était lancé et les futuristes et autres visionnaires étaient fin prêts pour proposer leur vision prospective à grands coups de disruption et de révolution.

Avec l'avènement du bitcoin et le tapage médiatique qui s'amplifiait autour de cette technologie disruptive, il aurait été difficile, pour les banques et les établissements financiers, de passer à côté du sujet. D'autant que la technologie blockchain semblait permettre des transactions instantanées à des coûts minimes et sans organe central de contrôle.

1. Philippe Herlin est économiste et auteur de *La Révolution du bitcoin et des monnaies complémentaires*.
2. http://www.lemonde.fr/economie/article/2015/09/30/la-revolution-blockchain-legs-du-bitcoin-en-version-seduction_4778603_3234.html
3. http://www.agefi.fr/banque-assurance/actualites/hebdo/20160218/blockchain-prochaine-revolution-159207

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

La technologie blockchain semblait être enfin prête pour révolutionner, entre autres, le monde de la banque grâce à une réduction des risques de contrepartie et donc des besoins en fonds propres, une réduction des coûts d'infrastructure réseau et informatiques et des économies de traitement de l'information (accessibilité, fiabilité).

L'analyse de Banco Santander

En juin 2015, Banco Santander notait dans son rapport « Fintech 2.0 » : « La technologie de la blockchain peut permettre aux banques d'économiser de 15 à 20 milliards de dollars (jusqu'à 17,9 milliards d'euros) par an d'ici à 2022 en coûts d'infrastructures liés aux paiements internationaux, au trading et à la mise en conformité[1]. »

Face à cette déferlante d'économies rapidement réalisables et à cette disruption probable, de très nombreuses banques ont rejoint la start-up R3CEV[2] (ou plus communément nommée R3) lancée en septembre 2015 et ce, afin d'engager des réflexions autour de la technologie et développer leur propre blockchain « privée »… sans la monnaie bitcoin et sa blockchain. Ainsi R3 lança sa solution Corda en avril 2016. Le consortium compte aujourd'hui (août 2016) plus de 50 membres banques.

Un consortium en forme de communauté de projet est le projet Hyperledger lancé en décembre 2015 et initié par la fondation Linux, IBM et surtout Digital Asset Holdings[3] qui apportera sa marque Hyperledger[4] dans la corbeille. Les acteurs

1. http://santanderinnoventures.com/fintech-2-0-paper-highlights-the-multi-billion-dollar-opportunity-open-to-financial-technology-businesses-which-can-help-to-reboot-financial-services/
2. R3CEV : http://r3cev.com/
3. Digital Asset Holdings : https://digitalasset.com/
4. Hyperledger : https://www.hyperledger.org/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

ayant rejoint ce projet sont : Accenture, ANZ Bank, Cisco, CLS, Credits, Deutsche Börse, DTCC, Fujitsu Limited, IC3, IBM, Intel, J.-P. Morgan, London Stock Exchange Group, Mitsubishi UFJ Financial Group, R3, State Street, SWIFT, VMware, Wells Fargo…

D'autres évolutions et cas d'usage ont suivi en France : « Nous allons profiter de l'ordonnance sur la réglementation financière, chargée de dépoussiérer les bons de caisse et créer des minibons[1], pour expérimenter sur la blockchain », déclarait Emmanuel Macron, ministre de l'Économie (juin 2016). Cette expérimentation, première du genre en France, permettra de démocratiser la technologie blockchain et de créer un premier cas d'usage.

Goldman Sachs a choisi de prendre le virage des Fintech

Un tiers des effectifs de l'entreprise est désormais constitué d'ingénieurs et de *data scientists* (soit plus de 12 000 profils techniques, près de la moitié des effectifs de Google). Lloyd Blankfein (PDG de Goldman Sachs) ne parle plus de banque, mais d'entreprise de technologie. Une partie de leur plateforme est passée à l'*open source*, mettant fin à la culture du culte du secret. Goldman Sachs soutient aussi le développement de Symphony, un système de messagerie secrète concurrent de la solution de Bloomberg, avec un argument massue : Symphony représente 1 % du coût de son concurrent. Enfin, nul besoin de préciser que Goldman Sachs place la blockchain au cœur de sa stratégie. La banque faisait d'ailleurs partie des neuf membres fondateurs de R3CEV en septembre 2015.

1. Minibons : https://bitcoin.fr/quelle-blockchain-pour-les-minibons/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Ainsi, promise à un bel avenir, l'influence de la blockchain s'étend déjà au-delà de la finance et l'assurance semble être une prochaine cible avant de s'étendre progressivement, ou rapidement (l'histoire nous le dira) à l'ensemble des pans de l'économie et de la société.

Quelques champs d'application

Découvrons brièvement quelques champs d'application[1] :

- finance (paiements instantanés et quasi gratuits entre les parties) ;
- assurance (microcontrats, micropaiements, assurance collaborative, gestion plus efficace de l'identification des clients et des données associées, certification de la provenance d'un bien) ;
- État (système de vote transparent et sécurisé, collecte des impôts, cadastres) ;
- e-commerce (paiement en ligne simple et sécurisé, plate-formes disruptives) ;
- Internet des objets ;
- industrie (gestion des objets connectés et autonomisation des objets pour réaliser des transactions) ;
- identité digitale ;
- logistique (gestion des processus et des contrats *via* des procédés algorithmiques) ;

1. Le lecteur trouvera une liste plus détaillée des diverses applications de la blockchain dans le chapitre 3 et en fin d'ouvrage la liste à jour à fin 2016 des principaux projets en cours de développement ou d'utilisation.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

- alimentation (traçabilité des informations attachées à un lot de plats préparés, de l'abattage à l'emballage) ;
- propriété intellectuelle des contenus (articles, photos, musiques, illustrations) ;
- transaction immobilière dans des pays où il n'y a pas de cadastre ;
- authentification d'œuvres, d'objets, de valeur ;
- enseignement (authentification des diplômes vérifiable par tous) ;
- santé (gestion de la traçabilité des médicaments, sécurisation des données de santé, gestion des données des patients) ;
- énergie (*smart grid*, *smart building*, *smart city*) ;
- covoiturage décentralisé.

La blockchain idéale pour les institutions financières et bancaires

Lors de la conférence Blockchain Vision[1] organisée par Finyear Group le 10 décembre 2015 à Paris, Luca Comparini, Blockchain Leader chez IBM France, a tenté de dégager les caractéristiques que devrait posséder une blockchain pour être utilisable par le secteur bancaire :

- une gestion de l'identité : il est indispensable dans un réseau *business to business* de pouvoir connaître l'identité de la contrepartie avec laquelle nous faisons une transaction ;
- un algorithme de consensus modulable : quand on connaît l'identité des participants, le *proof of work* est inutilement lent et dispendieux. Selon l'usage, il faudrait pouvoir changer d'algorithme de consensus (*proof of stake*, *proof of work*...) ;
- une confidentialité garantie : il ne faut pas que les transactions soient publiques ;

1. http://www.blockchain.vision

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

• un livre « auditable » : si les transactions doivent rester confidentielles, elles doivent cependant être accessibles au régulateur ;

• une blockchain « scalable » : la blockchain idéale doit pouvoir supporter un grand nombre de transactions. Cela soulève beaucoup de questions à l'heure actuelle ;

• une blockchain pérenne : les systèmes de paiement qui existent aujourd'hui ont été initiés il y a très longtemps. Si on invente un nouveau système, il faut qu'il puisse perdurer, ce qui signifie être capable d'anticiper des problèmes qui n'existent pas encore.

Pour IBM, la technologie blockchain en est donc à ses balbutiements et n'est pas encore adaptée aux besoins du secteur bancaire. Entre autres problèmes, celui de la « scalabilité » et de l'absence de confidentialité des transactions rend son utilisation impossible dans la plupart des cas, en l'état actuel des choses. Néanmoins, même si nous sommes toujours dans une phase initiale, les ingénieurs d'IBM ont déjà mené quelques réflexions qui ne se limitent pas au secteur bancaire, mais s'étendent « à tous les domaines B2B où IBM a une place et une compétence métier », affirme Luca Comparini.

Depuis décembre 2015, de très nombreux projets bancaires ont émergé et IBM propose désormais la solution Hyperledger[1] (que nous découvrirons au chapitre 4).

Nous pourrions toutefois ajouter un point important que l'on retrouve dans de nombreux projets bancaires où les acteurs sont multiples : l'interopérabilité des systèmes devra être garantie pour permettre l'harmonisation des échanges. Ce qui fait que, avec l'hétérogénéité des systèmes au sein des banques, la partie n'est pas gagnée...

1. http://www.ibm.com/blockchain/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Chapitre 2

La blockchain aujourd'hui

« Le secret du changement consiste
à concentrer son énergie pour créer du nouveau,
et non pas pour se battre contre l'ancien. »

Dan Millman

Copyright © 2017 Eyrolles.

Copyright © 2017 Eyrolles.

Voyons maintenant les différentes blockchains qui ont successivement émergé et donné naissance à l'écosystème que nous connaissons aujourd'hui. Pour cela, commençons par la blockchain Bitcoin et sa genèse.

La blockchain Bitcoin

Un peu d'histoire

À l'origine, la blockchain Bitcoin est une amélioration du concept b-money (imaginé par Wei Dai en 1999, où les serveurs étaient supposés verser un dépôt de garantie dans un mécanisme peu explicite) et bitgold (décrit en 2005 par Nick Szabo[1] qui avançait l'idée d'utiliser une chaîne de preuves de calcul).

Mais avant de poursuivre, deux définitions terminologiques pour la bonne compréhension des paragraphes à suivre :

- La *cryptographie asymétrique*[2], ou chiffrement à clé publique/clé privée, est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Le principe du chiffrement asymétrique est de disposer de deux clés (que l'utilisateur « fabrique » lui-même).
- Un *système distribué* est un ensemble d'entités autonomes de calcul (ordinateurs, PDA, processeurs, processus, processus léger, etc.) interconnectées et qui peuvent communiquer en réseau. Nous pourrions citer en exemple un réseau physique de machines avec plusieurs processus tournant sur une même machine.

1. Nick Szabo, informaticien, juriste et cryptographe, est connu pour ses travaux de recherche dans les contrats numériques et la monnaie numérique. Il est diplômé de sciences informatiques de l'université de Washington.
2. Voir glossaire : http://www.blockchaindailynews.com/glossary/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

1977 à 2005 : avant l'arrivée de Bitcoin et de son inventeur[1]

- 1977 : première description du chiffrement RSA[2] qui utilise une clé publique pour chiffrer des données confidentielles et une clé privée pour les déchiffrer.
- 1979 : Ralph Merkle[3] invente le mécanisme de compression par l'arbre de Merkle (ou « Merkle tree[4] compression mechanism »). Il est utilisé pour stocker et vérifier un grand volume de données efficacement et de manière sécurisée, et employé par le protocole Bitcoin pour calculer la racine de Merkle de toutes les transactions contenues dans un bloc de données.
- 1990 : le mathématicien américain David Chaum invente DigiCash[5], une monnaie électronique (centralisée et propriétaire) basée sur des protocoles cryptographiques.
- 1992 : Scott Vanstone (Certicom) propose l'algorithme ECDSA (Elliptic curve digital signature algorithm) qui utilise des clés plus courtes et permet des opérations de signature et de chiffrement plus rapides que la RSA.

1. https://bitcoin.fr/histoire/
2. RSA Security est une entreprise dont le sigle est formé à partir des noms de ses fondateurs : Ronald Rivest, Adi Shamir et Leonard Adleman. Ce sont les coinventeurs du cryptosystème à clé publique du même nom : le chiffrement RSA qui est un algorithme cryptographique de cryptographie asymétrique.
3. Ralph C. Merkle est un cryptographe américain et chercheur en nanotechnologies. Il est l'un des pionniers de la cryptographie asymétrique avec Martin Hellman et Whitfield Diffie. En 1974, il a créé les puzzles de Merkle, la première construction (non top secret) à clé publique (publication en 1978).
4. http://blogchaincafe.com/merkle-roots-et-merkle-trees-expliques#more-110
5. https://bitcoin.fr/pages/DigiCash

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

- 1994 : Nick Szabo avance l'idée de *smart contract* ou contrat intelligent (voir dans ce chapitre les pages consacrées à la blockchain Ethereum).
- 18 juin 1996 : la NSA publie un rapport intitulé « Comment produire de la monnaie : la cryptographie du cash électronique anonyme[1] ».
- 1997 : Adam Back[2] invente HashCash, un système de preuve de travail à partir d'une idée introduite par Cynthia Dwork et Moni Naor dans un rapport publié en 1993, *Pricing via Processing or Combatting Junk Mail*. Adam Back deviendra plus tard le premier interlocuteur de Satoshi Nakamoto.
- 1998 : faillite de DigiCash. Wei Dai lance l'idée d'un cash numérique basé sur un registre distribué sur la liste de diffusion The Cypherpunks.
- 1999 : Shawn Fanning invente, avec Napster, la technologie pair à pair, ou *peer-to-peer* (P2P) *technology*. La plateforme de partage de fichiers audio Napster fonctionnait avec un serveur central (*farm*) qui jouait le rôle d'un registre centralisé de tous les fichiers appartenant à, ou demandés par les pairs. Ce système centralisé constituait le point unique de défaillance (*Single Point of Failure*-SPOF) de Napster et le site a été fermé par le FBI en 2001 pour violation des droits de propriété intellectuelle.
- 2000 : Tom Pepper et Justin Frankel développent Gnutella, première plateforme de transfert de fichiers P2P complètement distribuée.
- De 1998 à 2005 : Nick Szabo[3] développe le projet BitGold[4], une monnaie numérique décentralisée basée sur des chaînes

1. https://bitcoin.fr/comment-produire-de-la-monnaie-la-cryptographie-du-cash-electronique-anonyme-2/
2. https://bitcoin.fr/Blockchain-et-Sidechains
3. https://bitcoin.fr/Le-retour-de-Nick-Szabo
4. http://unenumerated.blogspot.fr/2005/12/bit-gold.html

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

infalsifiables de preuves de travail et utilisant de nombreux éléments qu'on retrouvera dans Bitcoin : horodatage, signatures numériques, clés publiques… Le système se révèle cependant trop vulnérable aux attaques.

- 2004 : développement de Ripplepay, une tentative de système monétaire décentralisé.

2007 à 2010 : l'avènement de la blockchain Bitcoin et de sa devise bitcoin

Qui est Satoshi Nakamoto (中本哲史) ? Un peu d'histoire[1] :

- Depuis 2007, Satoshi Nakamoto, la mystérieuse figure qui se cache derrière l'invention de Bitcoin, a affirmé qu'il avait travaillé sur Bitcoin.
- 19 août 2008 : Satoshi Nakamoto réserve le nom de domaine bitcoin.org.
- 31 octobre 2008 : annonce de la naissance de Bitcoin (sur laquelle Satoshi Nakamoto travaille depuis 2007, selon ses propres affirmations). Il publie *Bitcoin : A Peer-to-Peer Electronic Cash System*[2]. Il y expose une méthode pour résoudre un problème cryptographique sur lequel achoppait la recherche depuis plusieurs décennies, le problème du double paiement ou problème des généraux byzantins (voir paragraphe dédié plus loin). Celui-ci empêchait à deux agents d'échanger des actifs, comme une monnaie par exemple, sans le passage par un tiers de confiance.
- 3 janvier 2009 : un premier bloc (*bloc genesis*) est créé.
- 12 janvier 2009 : première transaction bitcoin.

1. Retrouvez l'histoire du bitcoin sur : http://historyofbitcoin.org/ et sur https://bitcoin.fr/histoire/
2. http://www.finyear.com/Bitcoin-A-Peer-to-Peer-Electronic-Cash-System-by-Satoshi-Nakamoto_a34914.html

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

- Février 2009 : Satoshi Nakamoto diffuse la première version du logiciel Bitcoin sur le site P2P Foundation et crée les premiers bitcoins.
- 2009 et 2010 : Satoshi Nakamoto (ou le groupe de personnes que cache ce nom, à l'époque Satoshi n'est pas encore connu) conçoit et crée Bitcoin et le logiciel Bitcoin-Qt.
- Mi-2010 : les développeurs et la communauté Bitcoin perdent progressivement contact avec Satoshi Nakamoto.
- 12 décembre 2010 : un dernier message est posté par Nakamoto sur le forum Bitcointalk[1]. Peu de temps avant son évanescence, Nakamoto désigne Gavin Andresen comme son successeur en lui donnant accès au projet SourceForge Bitcoin et une copie de la clé d'alerte, une clé cryptographique privée unique permettant d'atténuer les effets d'une attaque potentielle sur le système Bitcoin – comme la découverte d'une faille cryptographique permettant de modifier *a posteriori* les transactions, ou la prise de contrôle de plus de 51 % des nœuds du réseau (voir l'encadré consacré à ce sujet plus loin dans ce chapitre). Les opérateurs des nœuds du réseau peuvent lors d'une alerte soit avertir leurs usagers, soit stopper tout enregistrement de transaction.

Définition

Le terme « bitcoin » provient de la contraction des termes anglais *bit*, unité d'information binaire, et *coin*, pièce de monnaie. Bitcoin[2] désigne à la fois un protocole informatique (Bitcoin) à travers le réseau internet et l'unité de compte (bitcoin) utilisée par ce système de paiement.

1. https://bitcoin.fr/satoshi-nakamoto
2. https://en.bitcoin.it/wiki/Main_Page

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

La blockchain Bitcoin est une technologie libre et ouverte qui fonctionne en réseau pair à pair (*peer-to-peer* ou P2P), sans autorité centrale (sans passer par une institution financière) et qui permet l'échange d'unités (bitcoin ou BTC) tout en enregistrant chaque transaction (horodatage) dans un grand livre de compte (*ledger*) dans lequel toute modification est impossible.

La gestion des transactions et la création de bitcoins sont prises en charge collectivement par le réseau et sa conception est publique ; personne ne possède ni ne contrôle la blockchain Bitcoin et chacun peut s'y joindre. Grâce à plusieurs de ses propriétés uniques, Bitcoin rend possible des usages prometteurs qui ne pourraient pas être couverts par les systèmes de paiement actuels.

La devise bitcoin, contrairement aux autres devises monétaires, n'est pas l'incarnation de l'autorité d'un État, d'une banque ou d'une entreprise et chaque bitcoin est identifiable dans un grand livre de compte par un historique de toutes les transactions dans lesquelles il est impliqué depuis sa création.

L'analyse de Pierre Noizat, CEO de Paymium

« Le bitcoin est une nouvelle monnaie numérique pour des transactions sans tiers de confiance : c'est de l'argent liquide sur Internet. À la différence des monnaies traditionnelles, bitcoin est une monnaie programmable… et fonctionne sans banque centrale : équipé d'un porte-monnaie bitcoin, vous pouvez être votre propre banque. »

Fonctionnement

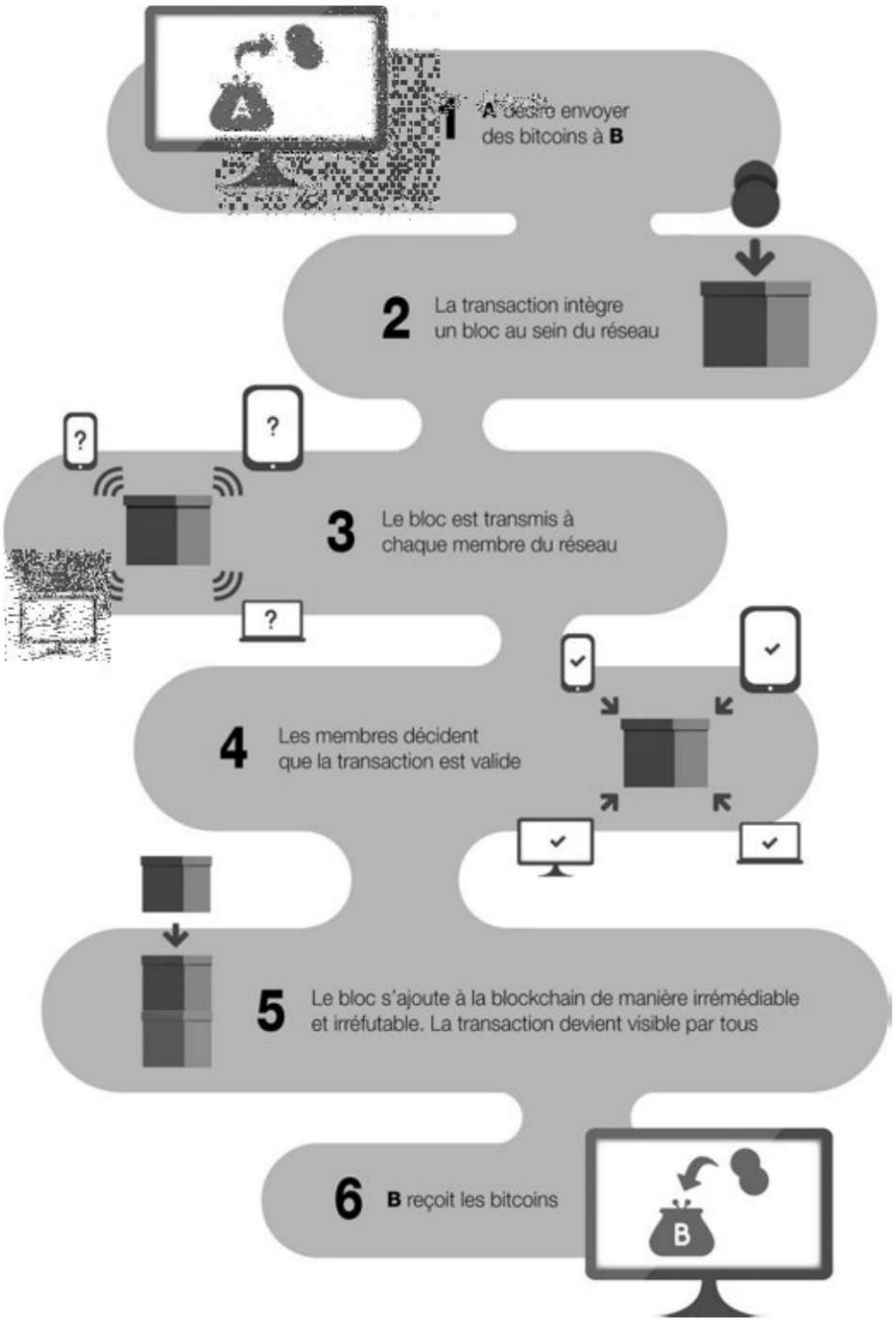
La blockchain Bitcoin repose sur un protocole cryptographique notamment pour :

- d'une part, résoudre le problème dit « de la double dépense », qui avait jusqu'alors empêché l'émergence d'un tel type de

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

monnaie (A donne à B en s'assurant qu'il n'a pas donné à C en parallèle) ;

- d'autre part, garantir l'impossibilité de falsifier les identifiants des parties prenantes et la valeur du stock de bitcoins figurant dans les porte-monnaie électroniques.



Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Le fonctionnement de la blockchain Bitcoin suit quatre étapes :

- deux personnes s'accordent sur une transaction ;
- grâce à la blockchain la transaction est encryptée et validée par consensus (*proof of work*/minage, voir ci-après) ;
- elle est ensuite inscrite puis verrouillée dans le dernier bloc de la blockchain ;
- enfin la blockchain est répliquée dans tous les nœuds (participants) du réseau.

Accès au réseau

Bitcoin est un réseau *peer-to-peer* : les participants forment un réseau pair à pair communiquant à travers Internet. Lorsqu'un ordinateur cherche à se connecter au réseau, sa première tâche consiste à trouver d'autres ordinateurs connectés.

Une fois l'ordinateur connecté, la deuxième étape consiste à télécharger la base de données de toutes les transactions effectuées depuis le lancement du projet, une transaction consistant en un transfert d'un certain montant de bitcoins d'un compte à un autre.

Un compte est identifié par une adresse bitcoin, qui schématiquement est analogue à un numéro de compte en banque.

L'analyse de Pierre Noizat

« Pour démarrer, le plus simple est donc de vendre un bien (par exemple des euros) ou un service contre des bitcoins. Paymium.com[1] est un site qui permet à des particuliers de s'échanger des devises (euros) contre des bitcoins : il y a des vendeurs et des acheteurs qui constituent une "place de marché".

1. Entre autres plateformes, voir la liste en fin d'ouvrage.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Pour acheter des bitcoins, il faut passer par trois étapes :

• Étape 1 : ouvrir un compte et faire un virement bancaire vers ce compte pour pouvoir échanger des euros contre des bitcoins. Le compte est maintenant approvisionné en euros après le délai pris par le virement bancaire.

• Étape 2 : consulter le carnet d'ordres pour voir à quels prix les bitcoins sont proposés par les vendeurs sur la place de marché.

• Étape 3 : passer un ordre d'achat (de bitcoins) au prix limite que vous souhaitez fixer. Si votre prix limite est inférieur au prix du meilleur vendeur, votre ordre ne sera pas exécuté tant qu'un vendeur ne proposera pas une offre inférieure ou égale à votre prix limite.

Votre ordre peut être exécuté partiellement si les vendeurs proposent une quantité inférieure à celle que vous demandez.

Votre ordre peut être exécuté immédiatement si votre prix limite est supérieur ou égal à celui proposé par le meilleur vendeur. »

Hormis les places de change, d'autres solutions existent[1] comme les plateformes de séquestre, les points de vente à sens unique et les changes physiques par distributeur automatique.

Comment acquérir des bitcoins ?

Dans la théorie, il est possible de trouver de nouveaux bitcoins grâce au « minage », c'est-à-dire en participant à la vérification des transactions mais, dans la pratique, ce n'est pas la méthode la plus simple car il faut installer un logiciel, certes gratuit, mais peu facile d'accès et d'utilisation pour un néophyte, et disposer d'une puissance de calcul importante (voir plus loin le paragraphe consacré au minage).

Donc le plus simple pour acquérir des bitcoins est de suivre la méthode et les solutions proposées par Pierre Noizat.

1. Acquérir des bitcoins : https://bitcoin.fr/obtenir-des-bitcoins/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Transactions

Pour être valide, chaque transaction doit être signée (au sens cryptographique du terme) en utilisant de la cryptographie asymétrique ou chiffrement à double clé (publique et privée).

Une transaction reçoit en entrée la référence d'une transaction précédente qui justifie que les fonds induits sont bien réels, et produit en sortie une ou plusieurs adresses bitcoin avec les montants attribués correspondants. Une transaction équilibre toujours ses entrées et ses sorties.

Toutefois, cette nouvelle transaction n'est pas immédiatement considérée comme globalement valide, car elle doit d'abord être incorporée dans le registre des transactions (la blockchain), qui est formé d'une suite de blocs de transactions. Les transactions, émises en clair, sont reconnues valables par les signatures cryptographiques correspondantes qui ainsi les avalisent.

Actuellement, le nombre de transactions par jour progresse très rapidement. Les volumes étaient d'environ 200 000 par jour en juin 2016 et presque 300 000 fin novembre 2016.

En revanche, en matière de nombre de transactions par seconde, la blockchain Bitcoin est moins performante que des technologies plus conventionnelles. Cela est souvent expliqué par le fait que le réseau Bitcoin est limité par sa conception, son ADN, à traiter au maximum environ sept transactions par seconde, alors que le réseau de paiement Visa a une capacité maximale de 56 000 transactions par seconde.

Porte-monnaie ou *wallet*

Contrairement aux institutions bancaires qui peuvent avoir plusieurs comptes par client, avec toutes les informations concernant l'historique de compte, il n'existe pas de compte pour les bitcoins. La blockchain garde bien une trace de chaque

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

transaction, mais elle ne tient pas le solde de compte pour ses utilisateurs. Il est par conséquent impossible de récupérer vos informations par ce biais.

Les utilisateurs ont un « porte-monnaie » ou *wallet*[1]. Ce dernier contient des « adresses numériques » associées à une paire de clés fonctionnant grâce au système de cryptage asymétrique (clé publique/clé privée). Notez que la clé privée est stockée dans le porte-monnaie et que la clé publique est enregistrée sur la blockchain et donc inviolable. Donc, comme dans la vraie vie, il ne faut pas perdre son porte-monnaie…

Perdre sa clé privée revient à perdre les bitcoins associés

C'est arrivé à James Howells, un Anglais qui avait acheté près de 7 500 bitcoins en 2009 (à l'époque la crypto-monnaie, très peu connue, ne valait presque rien). La clé associée à cette transaction était stockée sur son disque dur mais malheureusement pour lui, il l'a jeté après avoir renversé de la limonade sur son ordinateur. Lorsque le bitcoin a atteint 1 000 dollars, il détenait potentiellement 7,5 millions de dollars (ça fait cher la limonade…). Malheureusement, sans la clé il n'a jamais pu remettre la main sur ses bitcoins.

Valeur du bitcoin

Sa valeur est déterminée de façon entièrement flottante par l'usage économique qui en est fait et par le marché des changes. Les règles organisant l'émission monétaire sont déterminées uniquement par le code informatique libre du logiciel Bitcoin.

1. Voir glossaire : http://www.blockchaindailynews.com/glossary/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

L'analyse de Pierre Noizat[1]

« La valeur des bitcoins naît du consensus d'une communauté pour accepter les bitcoins comme valeur d'échange. C'est exactement le même cas pour les monnaies étatiques (*fiat money*) comme le dollar puisque, depuis 1973, elles ne sont plus adossées à un étalon or (*commodity money*) : la communauté nationale s'accorde donc pour reconnaître la valeur de billets sans attendre en échange la moindre possibilité de les convertir en or au guichet d'une banque, fût-elle une banque centrale. »

Lors de la création de la blockchain Bitcoin, son créateur Satoshi Nakamoto a inscrit dans le protocole (ensemble des règles qui définissent tout le fonctionnement du réseau) que seulement 21 millions de bitcoins seraient créés. Ce plafond aurait été décidé dans un esprit libertarien afin d'empêcher toute inflation sur la valeur du bitcoin.

Quelques unités du bitcoin :

- 1 bitcoin = 1 000 milli-bitcoin ;
- 1 bitcoin = 1 000 000 micro-bitcoin ou bits ;
- 1 bitcoin = 100 000 000 satoshi.

Le nombre de bitcoins est donc limité à 21 millions d'unités et chaque bitcoin est divisible jusqu'à la huitième décimale. Donc le plus petit montant qui puisse être transféré est de 0,00000001 (10^{-8}) bitcoin, nommé « satoshi » par la communauté Bitcoin, en hommage à l'inventeur de cette monnaie.

Notez que du 3 janvier 2009, date à laquelle sont apparus les 50 premiers bitcoins dans la transaction qui fixe l'origine temporelle de toutes les transactions suivantes, à fin novembre 2016, la valeur du bitcoin est passée de quasi 0 dollar américain à plus de 700 dollars américains[2].

1. « D'où vient la valeur des bitcoins ? », http://e-ducat.fr/links/value/
2. Source : https://blockchain.info/fr/charts/market-price?timespan=all

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Bitcoin : minage ou consensus

Dans la blockchain Bitcoin, pour ajouter une transaction et générer de nouveaux bitcoins, il faut engager un consensus que l'on nomme « le minage ».

Ce processus implique que des individus sont récompensés par le réseau pour leurs services. Les mineurs traitent les transactions et sécurisent le réseau en utilisant du matériel spécialisé et, en échange, collectent de nouveaux bitcoins.

Ainsi pour miner, certains utilisateurs (nœuds) mettent à contribution leur puissance de calcul informatique (les CPU[1]) afin de vérifier, d'enregistrer et de sécuriser les transactions dans la blockchain.

On peut définir le mécanisme comme une sorte de « *winner take all* », c'est-à-dire qu'à chaque transaction, des milliers de mineurs lancent des calculs mais un seul trouve la solution qui le valide.

Ainsi, pour être confirmé et enregistré sur le réseau, chaque bloc est le fruit d'un consensus machinique et algorithmique et ce processus est appelé *proof of work* (PoW) ou preuve de travail. Pour information, la difficulté change à chaque 2 016 blocs.

Le réseau essaie d'assigner la difficulté de telle sorte que la puissance de calcul mondiale prenne exactement 14 jours pour générer 2 016 blocs. C'est pourquoi la difficulté augmente de pair avec la puissance du réseau.

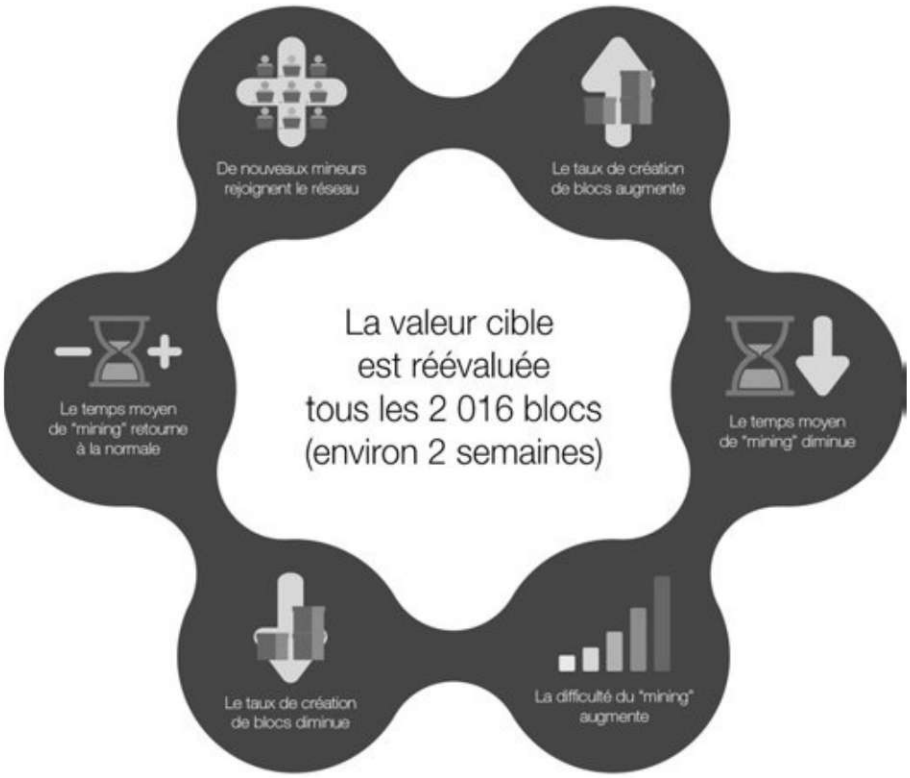
Le minage[2], protocole (algorithme[3]) de consensus distribué et décentralisé, consiste en un décryptage de données ou calcul

1. CPU : voir glossaire : http://www.blockchaindailynews.com/glossary/
2. Minage : une « mine » d'informations sur https://bitcoin.fr/minage/
3. Les algorithmes de hachage sont SHA-256 et RIPEMD-160. Un double hash en SHA-256 est utilisé pour obtenir le hash des blocs et donc la preuve de travail, tandis qu'un SHA-256 suivi d'un RIPEMD-160 est utilisé pour construire les adresses bitcoin.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

mathématique (c'est pour cela qu'on parle de crypto-devises ou crypto-monnaies, car pour arriver à les produire il faut passer par un processus de décryptage).

Arrivé à ce point de notre démonstration, il est important de préciser que les mineurs ne sont pas les seuls à vérifier les transactions. En effet, n'importe qui peut faire tourner Bitcoin Core[1] et vérifier que l'ensemble des transactions sont conformes. C'est la particularité du protocole Bitcoin et son point fort : permettre à chacun de vérifier que tout est parfaitement en règle.



1. Bitcoin Core est un projet *open source* qui maintient et publie le logiciel client Bitcoin dénommé « Bitcoin Core ». C'est un descendant direct du logiciel client Bitcoin originel créé par Satoshi Nakamoto suite à la publication du fameux livre blanc du Bitcoin. Il est téléchargeable ici : https://bitcoin.org/fr/telecharger

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

La question de la consommation énergétique

Bitcoin consomme beaucoup d'énergie. Le mécanisme de consensus le plus souvent utilisé dans les systèmes existants, le *proof of work* (preuve de travail), consomme une très grande quantité d'électricité pour fonctionner ; le réseau le plus important, Bitcoin, consommerait autant d'électricité que l'Irlande tout entière[1].

Depuis plusieurs années un certain nombre de chercheurs, mais également des journalistes ou des détracteurs de la blockchain Bitcoin, sont persuadés par le discours du lobby bancaire que le minage des bitcoins est un gaspillage énergétique[2]. Qu'en est-il vraiment ?

L'analyse de Pierre Noizat[3]

« La puissance de calcul totale du réseau est de 500 milliards de Mhash/s (à la date du 28 novembre 2015). L'efficacité du matériel de minage peut être estimée autour de 2 000 Mhash/J.

La consommation électrique totale du réseau Bitcoin, disponible dans le monde entier, se situe donc autour de 250 MJ/s = 250 Mwatt, c'est-à-dire l'équivalent de 100 000 maisons aux États-Unis.

À titre de comparaison, il existe environ 2 millions de distributeurs de billets de banque dans le monde, chacun consommant en moyenne 200 watts, même si les modèles les plus récents affichent une consommation théorique de 70 watts (source : diebold.com).

Au final, les seuls ATM (sans compter les réseaux et *data centers* auxquels ils sont connectés) consomment donc 400 Mwatts.

1. Minage et consommation électrique : https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf
2. Lire « Plaidoyer pour le Bitcoin » (http://www.scilogs.fr/complexites/plaidoyer-pour-le-bitcoin/) pour découvrir les fausses informations publiées par les médias et les banques en 2013 à propos du Bitcoin…
3. Pierre Noizat, e-ducat : http://e-ducat.fr/2015-11-28-cop21-et-blockchain/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Si l'impression des billets de banque sur papier de haute qualité et leur transport en camions blindés sont pris en compte, l'adoption de masse de Bitcoin comme cash électronique permettrait de diviser l'empreinte carbone des systèmes de paiement par trois ou quatre.

Avec un coût moyen de l'électricité aux États-Unis de 10 cents par kilowattheure en 2015, on obtient un coût de 25 000 US dollars pour 150 bitcoins générés par heure, soit un coût de "production" de 167 dollars par bitcoin (environ 157 €), environ la moitié du prix de marché des bitcoins à la même date. La différence correspond à la prime d'utilité, présente et future, attribuée aux bitcoins. »

Le problème des généraux byzantins

Définition

Le problème ou « théorie des généraux byzantins » est une métaphore mathématique qui traite de la remise en cause de la fiabilité des transmissions et de l'intégrité des interlocuteurs. Il s'agit de savoir comment, et dans quelle mesure, il est possible d'accepter une information dont la source ou le canal de transmission est suspect.

Pour résoudre ce problème, nous devons utiliser une stratégie adaptée (en l'occurrence un algorithme). Ce problème a été traité en profondeur pour la première fois dans l'article « The Byzantine Generals Problem » publié en 1982[1].

Blockchain et problème des généraux byzantins

Voici comment se présente le problème : des généraux disposant chacun d'une armée doivent se coordonner pour assiéger une ville. Les généraux communiquent *via* des messagers fiables. Mais certains généraux sont des traîtres et visent à faire échouer le plan d'attaque (une faute byzantine est donc une

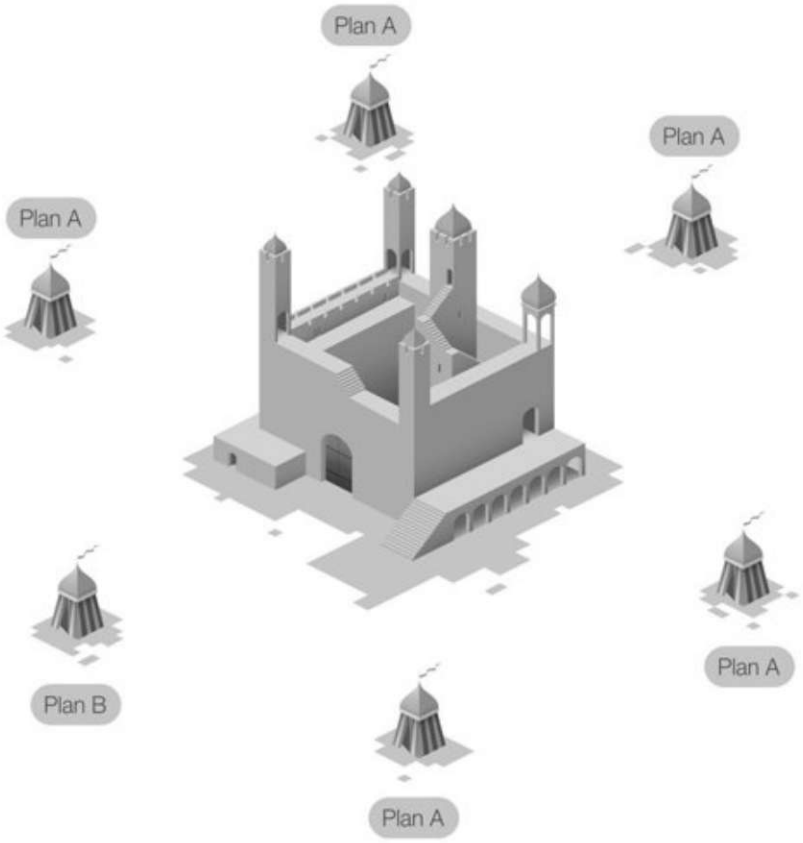
1. « The Byzantine Generals Problem », *ACM Transactions on Programming Languages and Systems*, vol. 4, n° 3, juillet 1982.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

défaillance qui consiste en la présentation d'informations erronées ou incohérentes.) Or, l'attaque ne peut avoir lieu que si les généraux arrivent à un consensus.

Problème des généraux byzantins



«Des généraux de l'armée byzantine campent autour d'une cité ennemie. Ils ne peuvent communiquer qu'à l'aide de messagers et doivent établir un plan de bataille commun, faute de quoi la défaite sera inévitable. Cependant, un certain nombre de ces généraux peuvent s'avérer être des traîtres, qui essaieront donc de semer la confusion parmi les autres. Le problème est donc de trouver un algorithme pour s'assurer que les généraux loyaux arrivent tout de même à se mettre d'accord sur un plan de bataille.»

Il faut donc trouver un algorithme pour s'assurer que les généraux loyaux arrivent tout de même à se mettre d'accord sur un plan de bataille. On doit coordonner la confiance en ayant

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

recours à des messages écrits et signés (non falsifiables) entre les généraux et en partageant des intentions entre tous les généraux. Et c'est là où nous revenons au consensus *proof of work*.

Les technologies blockchain représentent la première et peut-être la seule solution au problème des généraux byzantins et il est ainsi possible pour la première fois dans l'histoire de l'humanité de maintenir un registre qui soit à la fois ouvert au grand public et suffisamment sécurisé.

L'analyse d'Hubert de Vauplane[1]

« Comment la blockchain permet-elle d'établir une confiance (théoriquement sans faille) entre deux membres étrangers du réseau ? Ce problème mathématique, aussi appelé « problème des généraux byzantins », consiste à s'assurer qu'un ensemble de composants informatiques fonctionnant de concert sache gérer des défaillances ou malveillances.

Le système doit être capable de maintenir sa fiabilité dans le cas où une part minoritaire des composants enverrait des informations erronées ou malveillantes pour contourner la vérification de la double dépense (fraude). Pour résoudre cette difficulté, le protocole utilise un système cryptographique fondé sur un système décentralisé de preuves : la résolution de la preuve nécessite une puissance de calcul informatique élevée, fournie par les "mineurs".

Les mineurs sont des agents dont la fonction est d'alimenter le réseau en puissance de calcul, afin de permettre la mise à jour de la base de données décentralisée (liste des transactions dans le cas du bitcoin). Pour mettre à jour la base de données, les mineurs doivent confirmer les nouveaux « blocs » en décryptant les données (travail classique de cryptographie). Plus les mineurs sont nombreux, plus la résolution des preuves est difficile à s'attribuer.

Ainsi, le protocole peut devenir quasi inviolable dès lors que la concurrence est forte à chaque nœud du réseau, c'est-à-dire qu'aucun groupement de mineurs ne devient majoritaire. »

1. Extrait d'un article d'Hubert de Vauplane publié sur Finyear.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

L'algorithme des généraux byzantins[1] ou la tolérance aux pannes

La tolérance aux pannes byzantines ou *Byzantine Fault Tolerance* (BFT) est la capacité à tolérer des machines de façon arbitraire et à permettre à un système de continuer à fonctionner, éventuellement de manière réduite, sans tomber complètement en panne, lorsque l'un de ses composants ne fonctionne plus correctement.

Historiquement, ce sont les militaires, pendant la guerre froide, qui ont développé cette tolérance aux pannes afin de garantir la continuité des communications sur un réseau maillé, en l'occurrence le réseau ARPA[2].

Informatiquement parlant, et puisque les algorithmes ne sont pas nés avec la technologie blockchain, mais dans les années 1970, le problème des généraux byzantins est une représentation abstraite d'une classe de programmes mettant en œuvre plusieurs intervenants comme des processeurs dans un ordinateur, des ordinateurs dans un réseau, des robots dans une usine ou des nœuds dans une chaîne (avec ou sans blocs).

Ainsi dans le domaine de l'informatique distribuée, et en particulier dans les blockchains, la réponse à cette tolérance aux pannes sera apportée par Paxos[3] et Tendermint[4], qui sont des familles de protocoles permettant de résoudre le consensus

1. M. Correia, G.S. Veronese, N.F. Neves et P. Verissimo, « Byzantine consensus in asynchronous message-passing systems : a survey », *International Journal of Critical Computer-Based Systems*, vol. 2, n° 2, 2011, p. 141–161.
2. Ancien nom de la DARPA (Defense Advanced Research Projects Agency), l'agence du département de la Défense des États-Unis chargée des nouvelles technologies militaires et à l'initiative de ARPAnet.
3. Paxos est un algorithme qui résout le consensus dans les systèmes répartis par passage de messages en deux étapes de communication.
4. https://tendermint.com/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

dans un réseau de nœuds faillibles, c'est-à-dire susceptible d'avoir des pannes.

L'analyse de l'éditeur Tendermint

« La technologie blockchain est simplement une reformulation de BFT dans un contexte plus moderne tout en mettant l'accent sur la mise en réseau *peer-to-peer* et l'authentification cryptographique. Le nom dérive de la façon dont les transactions sont groupées en blocs, chaque bloc contenant un hachage cryptographique du précédent, formant une chaîne. En pratique, la structure de données de blocs de chaînes optimise la conception de BFT. »

Bitcoin : mineurs et rémunération

En théorie, tout le monde peut être mineur, ce qui était le cas au démarrage de la blockchain. Mais en pratique, avec le développement exponentiel des transactions, le minage est l'affaire de véritables entreprises essentiellement basées dans des zones géographiques où le coût de l'électricité est (quasiment) nul.

Dans la blockchain Bitcoin, un bloc contient actuellement 1 000 transactions avec une taille limite de 1 mégaoctet (la taille moyenne des blocs échangés oscille entre 600 et 700 ko) soit environ sept transactions par seconde. Quand le mineur arrive à confirmer un bloc de transactions, il remporte les 25 nouveaux bitcoins qui se créent toutes les dix minutes.

La blockchain Bitcoin existant depuis janvier 2009, la récompense pour la résolution d'un bloc était à l'origine de 50 bitcoins, mais elle est automatiquement divisée par deux tous les 210 000 blocs (environ tous les quatre ans) : les mineurs reçoivent aujourd'hui 25 bitcoins par bloc, 12,5 BTC à partir de 2017 puis 6,75 BTC à partir de 2021, etc.

Aujourd'hui, une poignée de mega-pools (GHASH. IO, AntPool, BW.COM, F2Pool…) ont le monopole de l'extraction de

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

bitcoins[1]. Il suffit de regarder sur le site blockchain.info dans la colonne « Relayé par » quel est le pool qui a réussi l'exploit de casser les derniers blocs (les chiffres sont exprimés en pourcentage).

L'attaque à 51 %[2]

Une attaque à 51 % survient lorsqu'un individu ou groupe d'individus contrôle plus de la moitié de la puissance de calcul dédiée au minage. Il peut alors refuser ou valider des transactions, et effectuer des doubles dépenses[3]. En effet, les nœuds du réseau (dans la blockchain Bitcoin, par exemple) reconnaissent comme légitime la chaîne la plus longue, qui sera statistiquement écrite par le groupe de mineurs qui possède la plus grande puissance de calcul.

Si une telle attaque avait lieu, il est fort probable que le réseau s'en rendrait compte rapidement.

Actuellement, la majeure partie de la puissance de calcul dédiée au minage est détenue par les pools (AntPool, F2Pool, BTCC Pool, Bit Fury). Si ces pools se mettaient d'accord, ils pourraient réaliser l'attaque ; ce qu'ils ne s'aventurent pas à faire car un piratage ferait chuter le prix de la monnaie, dont ils détiennent d'importants stocks.

Attention toutefois, nombre de cryptologues font remarquer à juste titre qu'un groupe d'individus capable de hacker plusieurs pools en même temps pourrait mener l'attaque.

---

1. Lire également « La tyrannie des mineurs », http://www.blockchaindailynews.com/La-Tyrannie-des-Mineurs_a24751.html
2. Pour en savoir plus, vous pouvez vous rendre sur le forum dédié : http://bitcoin.stackexchange.com/questions/658/what-can-an-attacker-with-51-of-hash-power-do
3. Si un utilisateur mal intentionné essaie de dépenser ses bitcoins auprès de deux destinataires différents au même moment, il s'agit d'une double dépense. Le minage et la chaîne de blocs existent pour créer un consensus dans le réseau afin de décider laquelle des deux transactions sera confirmée et considérée valide. (Voir glossaire : http://www.blockchaindailynews.com/glossary/)

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Une telle attaque n'est donc réalisable que par un État ou une grande entreprise (banque, hedge fund hostile...). En effet, le coût de la puissance de calcul et de l'énergie nécessaire est prohibitif : en février 2016, la puissance totale du bitcoin était de 1,2 million de Téra Hash[1] ! Sachant que le Téra Hash coûte environ 4 000 $, il ne faudrait pas moins de 4,8 milliards de dollars américains pour obtenir une telle puissance. Enfin, si la sécurité du réseau était compromise, une procédure d'urgence existe[2].

Blockchain et anonymat[3]

Le faux problème de l'anonymat

On reproche fréquemment au bitcoin d'être anonyme. Avoir de l'argent numérique décentralisé, de l'or digital, est fascinant et intéresse de nombreux acteurs économiques, mais la crainte d'ouvrir la voie à toutes sortes d'activités illicites couvertes par l'anonymat reste, à tort ou à raison, l'un des freins à l'adoption.

En analysant la question sous un angle plus technique, on comprend toutefois que cette appréhension peut être largement atténuée : le bitcoin n'est pas si anonyme qu'il en a l'air… Si d'un côté, nous n'avons pas besoin de fournir des informations d'identité pour créer un portefeuille ou envoyer une transaction, d'un autre côté, tout ce qui se passe dans la blockchain Bitcoin est en clair, ce qui rend les transactions publiquement traçables. Tout le monde peut ainsi créer un explorateur

1. La puissance de calcul d'un mineur est exprimée en Hash/s (quantité de hash calculée à la seconde) (Kilo Hash / Mega Hash / Giga Hash / Terra Hash).
2. Procédure suite à une attaque : https://en.bitcoin.it/wiki/Contingency_plans
3. Note rédigée par David Teruzzi (voir page de remerciements).

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

des données blockchain, comme le fait par exemple le site blockchain.info[1] (voir acteurs en fin d'ouvrage).

Les adresses bitcoin ne sont pas, elles-mêmes, reliées à une personne ou à une entité, c'est la raison pour laquelle on dit que le bitcoin est anonyme ou plutôt, pseudonyme. En effet, sur le réseau Bitcoin, l'identité de l'utilisateur est masquée derrière un pseudonyme cryptographique, qui peut être modifié à volonté. Les transactions sont signées avec ce pseudonyme et sont diffusées sur le réseau public pour vérifier leur authenticité et attribuer les bitcoins au nouveau propriétaire.

Cependant, l'identité d'une personne peut être associée à une adresse bitcoin par d'autres moyens. Lorsque cela se produit, on peut reconstruire les actions de cette personne dans le passé suivant l'historique blockchain. Une violation de l'anonymat individuel ponctuelle peut aller jusqu'à révéler l'ensemble des transactions bitcoin d'un individu.

Si dans une transaction, votre interlocuteur est un particulier qui vous connaît, celui-ci peut tenter de déduire, à partir des données publiques, le solde de votre portefeuille. Si dans une transaction, votre interlocuteur est un organisme (banque, État, réseau social…) auquel vous êtes tenu de fournir une identification, c'est encore pire : il connaît déjà votre identité et a les moyens informatiques de croiser ses informations avec votre empreinte digitale blockchain. Ainsi, si vous payez en bitcoin une paire de chaussures sur un site en livrant votre identité, vous donnez à ce site la possibilité d'aller lire dans la blockchain que trois transactions plus tôt vous avez loué une voiture, et six transactions plus tôt une chambre d'hôtel (bien sûr, à condition de connaître aussi la vraie identité bitcoin des deux vendeurs). Ce sont des informations qu'un circuit de

1. http://www.blockchain.info

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

carte bancaire détient déjà, par exemple, mais que vous ne voulez pas forcément partager avec celui qui vous a vendu votre dernière paire de baskets.

Ainsi, pendant que l'imaginaire collectif bute contre un problème largement surestimé, l'anonymat du bitcoin, les experts recherchent la manière de rendre vraiment anonyme une blockchain.

Il est vrai que le bitcoin ne respecte pas le processus *Know-Your-Customer* (KYC) (qui consiste en ce qu'une entreprise vérifie l'identité de ses clients) et que l'on peut ouvrir autant de portefeuilles que l'on veut sans déclarer son identité. Mais cela ne veut pas dire que le bitcoin soit 100 % anonyme (ou plutôt pseudonyme) dans la vie de tous les jours, à cause d'une de ses caractéristiques principales : la traçabilité.

Traçabilité et opacité

Presque toutes les crypto-monnaies existantes utilisent une blockchain transparente et seulement une petite minorité de projets ont pour cible de la rendre opaque. Dash[1], par exemple, qui contrairement au bitcoin utilise une architecture client-serveur qui fonctionne en *proof of work* de la même manière que le bitcoin, et raisonne plus en mode *proof of stake* en créant un sous-réseau composé de serveurs spéciaux (*masternodes*) qui fournissent des fonctionnalités supplémentaires telles que les transactions instantanées, et surtout les transactions privées (*darksend*). L'idée de base est que les transactions deviennent opaques en mélangeant l'argent qui est envoyé sur

1. Dash (anciennement connue sous le nom de Darkcoin) est une crypto-monnaie créée en 2012 par Evan Duffield, et présentée au grand public le 18 janvier 2014. Son nom initial, Darkcoin, a été changé le 25 mars 2015 en Dash, mot-valise de *digital* et de *cash*, c'est-à-dire « argent liquide numérique ».Voir https://www.dash.org/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

les *masternodes*. Dash est plus anonyme que le bitcoin, mais n'est pas en mesure d'assurer une opacité totale.

Zerocoin[1], puis ZeroCash Project[2], a été un autre projet de ce genre. L'idée étant d'envoyer des bitcoins dans le réseau Zerocoin et de les récupérer anonymisés dans le protocole. Cette idée a ensuite évolué jusqu'à donner Zcash[3] : une monnaie qui permet des échanges de base transparents avec l'option de les rendre anonymes avant une dépense grâce à un passage dans leur mélangeur interne, une sorte de *blackbox* qui assurerait l'opacité. Zcash est basée sur une cryptographie dite *zero-knowledge proof*.

Le projet Monero

Dans le domaine de l'anonymisation totale, le projet le plus abouti à ce jour est Monero[4].

Monero (qui signifie « monnaie » en espéranto) a deux propriétés :

- il permet d'envoyer et de recevoir des fonds sans que les transactions soient visibles publiquement ;
- il crée une ambiguïté qui rend virtuellement impossible de tracer les fonds dépensés.

Le protocole Monero utilise un procédé dit de signature de cercle[5] ponctuel (*one-time ring signatures*), une technologie d'anonymisation très puissante pour masquer les transactions.

Quand on crée une transaction, on en sélectionne aléatoirement d'autres dans la blockchain et on les signe en anneau

1. http://zerocoin.org/
2. http://zerocash-project.org/
3. https://z.cash/
4. https://getmonero.org/
5. Voir glossaire : http://www.blockchaindailynews.com/glossary/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

pour produire l'empreinte digitale à publier. Cette empreinte caractérisant la transaction est appelée *key-image*. Cette astuce cache aux observateurs le véritable signataire tout en garantissant que la transaction est sans aucun doute valide et qu'elle ne fait pas l'objet d'une double dépense.

Grâce aux *view-keys*, il est également impossible d'identifier le destinataire d'un paiement. Une transaction n'est pas envoyée à une clé publique, mais à une adresse à utiliser une seule et unique fois. Seul le destinataire en possession de la bonne *view-key* a un droit de lecture sur la transaction qui lui est destinée. Les transactions en clair étant interdites dans Monero, l'opacité est totale et la traçabilité absente. Et Monero pousse le vice jusqu'à vouloir cacher dans une prochaine mise à jour le montant même des transactions !

Avec la blockchain, lentement mais sûrement, l'argent fait sa mutation.

Reste à savoir comment le régulateur va réagir, étant donné que le bitcoin est toléré depuis 2009 sans qu'il respecte vraiment la loi en vigueur dans aucun des pays où il est utilisé. Que va-t-il se passer si une monnaie comme Monero se répand mondialement de manière non négligeable ? Pour l'instant, sa capitalisation dépasse les 100 millions de dollars, une goutte d'eau dans l'économie mondiale, mais il est intéressant de savoir que Microsoft l'a intégré au printemps 2016 dans son service BaaS (Blockchain-as-a-service).

Il va de soi que Monero, tout comme le bitcoin, ne peut garantir l'anonymat que dans la mesure où l'on reste à l'intérieur du système. S'il n'y avait plus aucune autre monnaie que Monero dans le monde, tous les paiements seraient anonymes. En revanche, à chaque utilisation de Monero pour des échanges vers d'autres monnaies transparentes (fiat ou crypto) on retombe dans le niveau de confidentialité propre à la monnaie

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

en question. Il est déconseillé d'entrer ou sortir du système Monero si l'on veut rester anonyme.

Sur la base de ces informations, vous comprenez qu'un dealer qui voudrait placer de l'argent illicite dans une crypto-monnaie y réfléchirait plus d'une fois avant de passer à l'acte. Et après la prise de décision, il y a fort à parier qu'il ne dormirait plus très bien la nuit : en effet, comment va-t-il sortir son argent du système, alors qu'il lui suffit d'en transférer une infime quantité vers un compte bancaire en dollars, pour laisser une trace de son identité sur un serveur quelque part dans le monde ?

Évolution, scalabilité

La scalabilité est la capacité qu'a un système à s'adapter à un changement d'échelle, en particulier sa capacité à maintenir ses fonctionnalités et ses performances en cas de forte demande… Le problème de certaines blockchains « classiques » est l'accroissement exponentiel des ressources techniques, économiques, énergétiques nécessaires pour réaliser certaines tâches. Exemple : beAchain, par son protocole spécifique de consensus/validation, est 100 % scalable.

Quid de la scalabilité[1] de la blockchain Bitcoin et de son évolution ?

À la lecture des capacités techniques de la blockchain Bitcoin, nous voyons bien que nous avons affaire à une technologie robuste qui a maintenant fait ses preuves et qui est très largement partagée dans le monde. Comment faire pour que nous puissions envisager des cas d'usage toujours plus divers et variés tout en maintenant son niveau de performance ? Comment réaliser une multitude de micropaiements sans perturber son

1. https://www.oreilly.com/ideas/blockchain-scalability

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

fonctionnement ? Comment améliorer les temps de réponse si nous envisageons des milliers de transactions à l'instar de ce que réalisent des opérateurs de paiement par carte bancaire, par exemple[1] ?

À partir de ces questions et donc des problématiques qui en découlent, nous avons vu cinq solutions apparaître :

- les altcoins ;
- l'augmentation de la taille des blocs de transactions ;
- les « sidechains » ou chaînes collatérales ;
- le « Lightning Network » ;
- les « side databases » ou blockchain databases.

Les altcoins[2] ou les « *alternative cryptocurrencies* »

À ce jour, plus de 700 crypto-monnaies[3], qui s'appuient sur leur propre blockchain ou sur celle de Bitcoin ou d'Ethereum, sont désormais disponibles, chacune d'elles se spécialisant dans un service ou une fonction spécifique.

Au 27 décembre 2016, le chiffre global est de 708 crypto-monnaies[4] (ou monnaies virtuelles).

1. Sur ce point, voir plus loin les paragraphes consacrés au « Lightning Network ».
2. http://altcoins.com/
3. Monnaie virtuelle interne à une blockchain permettant des transferts de valeurs de compte à compte. C'est une forme de monnaie numérique basée sur les mathématiques, où les techniques de cryptage sont utilisées pour réguler la production d'unités de la monnaie et vérifier le transfert de fonds. En outre, les crypto-monnaies fonctionnent indépendamment d'une banque centrale.
4. Source CoinMarketCap : http://coinmarketcap.com/all/views/all/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Ci-dessous, un classement des dix premières crypto-monnaies et leur valeur en euros au 9 décembre 2016 (source CoinMarketCap).

	Nom	Symbole	Capitalisation (euros)	Prix (euros)
1	Bitcoin	BTC	11 641 663 699	726,12
2	Ethereum	ETH	681 588 294	7,86
3	Ripple	XRP	240 950 923	0,006694
4	Litecoin	LTC	170 257 496	3,49
5	Monero	XMR	100 669 561	7,45
6	Ethereum Classic	ETC	65 912 772	0,760533
7	Dash	DASH	57 435 907	8,27
8	Steem	STEEM	50 380 602	0,222937
9	Augur	REP	34 324 776	3,12
10	NEM	XEM	27 572 820	0,003064

Le site CoinMarketCap.com permet de suivre le marché de la crypto-monnaie et l'on constate que la valeur de ces devises reste au final très faible comparée au volume global des échanges internationaux en devises fiat[1] (ou monnaies décrétées par l'État).

La Suède teste la monnaie numérique e-Krona

En Europe, les premiers billets de banque émis par un établissement bancaire (*stricto sensu*) sont apparus au début du XVII^e siècle avec la Banque de Stockholm en 1658. En 1668, la Banque de Suède (Riksbank[2]) succéda à la Banque de Stockholm qui fit faillite.

1. http://www.wikiberal.org/wiki/Monnaie-fiat
2. http://www.riksbank.se/en/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Aujourd'hui, et 358 ans plus tard, la Riksbank, la banque centrale la plus ancienne au monde, lance un projet pour examiner ce qu'est une monnaie numérique soutenue par une banque centrale et quels défis cela poserait. Elle espère prendre une décision sur l'opportunité de démarrer l'émission de ce qu'elle appelle un e-krona dans les deux prochaines années.

« C'est aussi révolutionnaire que le billet papier il y a plus de 300 ans. Qu'est-ce que cela signifie pour la politique monétaire et la stabilité financière ? Comment pouvons-nous concevoir ce projet : *via* une carte rechargeable, une application ou une autre manière de pratiquer ? », a déclaré C. Skingsley, gouverneur adjoint à la Riksbank au *Financial Times*.

Les banques centrales du monde entier ont seulement commencé à envisager les avantages potentiels et les défis découlant des devises numériques telles que bitcoin et la Suède considère que le lancement de e-krona conduirait sur le chemin d'une « société sans cash ». Ainsi, la banque centrale commence-t-elle à évaluer les implications technologiques, juridiques et politiques de cette monnaie électronique.

Les enquêtes de la banque centrale indiquent que moins de 15 % des Suédois effectuent la plupart des paiements en espèces. Et l'économie en espèces représente seulement 2 % du PIB de la Suède, contre 10 % en 1990. Il y a maintenant des entreprises en Suède qui n'acceptent pas les paiements en espèces. Même les sans-abri suédois vendent leurs magazines avec des terminaux de cartes bancaires.

En 2014, quatre paiements sur cinq étaient effectués par voie électronique, comparativement à une transaction sur quatre en Italie, l'Europe du Sud tendant à être plus orientée vers les paiements en espèces.

Il a été suggéré que la Suède pourrait devenir une société sans numéraire d'ici 2030 et Riksbank pourrait devenir la première banque centrale du monde à lancer sa propre monnaie virtuelle.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Les différentes crypto-monnaies

Parmi les crypto-monnaies, on peut citer :

- Litecoin[1] (quatrième crypto-devise en termes de capitalisation avec plus de 170 millions d'euros de capitalisation boursière).
- Namecoin[2], qui offre la possibilité de créer un réseau de noms de domaine décentralisé basé sur la technologie des blockchains. Un des buts de Namecoin est la mise en place d'un système d'adresses pour les ordinateurs connectés au réseau internet qui pourrait se substituer au système actuel DNS (Domaine Name System) en partie aux mains d'organisations américaines. La solution adoptée est le principe du premier arrivé, premier servi, où le premier enregistrement réussit tandis que le second échoue – un problème parfaitement adapté au protocole de consensus Bitcoin. Namecoin est la mise en œuvre la plus ancienne et la plus réussie d'un système d'enregistrement de noms basé sur une telle idée.
- OneCoin[3] est la première et unique crypto-monnaie au monde à stocker des documents *Know-Your-Customer* (KYC) sur sa blockchain dans un but de totale transparence. En deux ans (2014-2016), OneCoin est devenue l'une des monnaies virtuelles les plus importantes sur le marché, visant à devenir la première crypto-monnaie grand public mondiale. En plus de créer une monnaie stable, conforme à toutes les réglementations, OneCoin a bâti un écosystème autour de sa monnaie afin d'accroître son utilisabilité.
- Des crypto-devises communautaires comme Potcoin[4] et Mazacoin[5].

1. https://litecoin.org/fr/
2. https://namecoin.org/ et https://wiki.namecoin.org/indexphp?title=Welcome
3. http://www.onecoin.eu/
4. http://www.potcoin.com/
5. http://mazacoin.org/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

- Des projets très prometteurs comme BitShares[1], Dash[2] (ex-Darkcoin), Blackcoin[3], Viacoin[4], très récemment Zcash[5], etc.

Conscoin, une crypto-monnaie éthique dotée d'une conscience

Cette crypto-monnaie présente des atouts disruptifs. En effet, Conscoin est une crypto-monnaie autonome éthique et guidée, rien que cela...

Fin 2015, un groupe de chercheurs de l'université de Georgetown à Washington DC[6] a publié un document[7] proposant une nouvelle crypto-monnaie qui utilise l'intelligence artificielle (AI) pour développer une monnaie possédant un groupe prédéfini de principes éthiques afin de gouverner ses dépenses.

Ils précisent que les crypto-monnaies comme bitcoin offrent de nouvelles voies pour l'autonomisation économique des individus à travers le monde[8]. Cependant, elles fournissent également un outil puissant qui facilite les activités criminelles et qui causent beaucoup de tort aux individus et aux communautés. Ainsi, les défenseurs de la crypto-monnaie ont fait valoir que les dimensions éthiques de la crypto-monnaie

1. https://bitshares.org/
2. https://www.dash.org/
3. http://blackcoin.co/fr/
4. https://viacoin.org/
5. https://z.cash/ – Voir également : http://www.blockchaindailynews.com/What-is-Zcash_a24678.html
6. https://www.georgetown.edu/
7. « Cryptocurrency with a Conscience : Using Artificial Intelligence to Develop Money that Advances Human Ethical Values », http://www.finyear.com/attachment/641777/
8. «Virtual Currencies; Bitcoin & What Now after Liberty Reserve, Silk Road, and Mt. Gox? », https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2393537

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

ne sont pas qualitativement nouvelles, dans la mesure où l'argent a toujours été compris comme un instrument passif qui manque de valeurs éthiques et peut être utilisé à de bonnes ou de mauvaises fins.

Le groupe de chercheurs conteste la présomption que l'argent doit avoir une valeur neutre. En effet, en bâtissant sur les progrès de l'intelligence artificielle, de la cryptographie, et des machines éthiques, il soutient qu'il est possible de concevoir des crypto-monnaies artificiellement intelligentes, qui ne sont pas éthiquement neutres, mais qui régulent de manière autonome leur propre usage d'une manière qui reflète les valeurs éthiques de certains êtres humains, ou de sociétés humaines entières.

Pour ce faire, ces chercheurs proposent de fixer un cadre technologique pour ces crypto-monnaies puis d'analyser les implications juridiques, éthiques et économiques de leur utilisation. Ils suggèrent également que le développement de crypto-monnaies possédant de l'éthique ainsi que de la valeur monétaire peut permettre aux êtres humains disposant de nouveaux moyens économiques d'influer positivement sur l'éthique et les valeurs de leurs sociétés.

Cette crypto-monnaie autonome éthique et guidée (Autonomous Ethically Guided Cryptocurrency, AEGC) représente une forme d'application qui comprend deux traits distinctifs :

- la possession d'une forme d'intelligence artificielle qui permet de surveiller l'environnement, de recueillir et analyser les informations et de prendre des décisions autonomes guidées par des principes éthiques spécifiques ;
- le fonctionnement comme une crypto-monnaie qui peut être qualifiée d'un moyen d'échange et d'un jeton (*token*) pour le stockage de la valeur.

En combinant la technologie de la blockchain avec des formes particulières d'intelligence artificielle, on peut concevoir une crypto-monnaie qui peut examiner les circonstances associées à une transaction financière particulière, dans laquelle l'individu propriétaire de la crypto-monnaie serait susceptible d'engager et de formuler une décision de permettre ou non l'utilisation de la crypto-monnaie dans la transaction en question.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Pendant le processus de détermination, à savoir si oui ou non une transaction est autorisée, le logiciel d'intelligence artificielle de la crypto-monnaie ne cible pas les aspects financiers de la transaction. Au lieu de cela, il identifie et analyse le contexte éthique de la transaction pour conclure.

Cette innovation peut nous transporter loin du monde des « données intelligentes » (*smart data*) vers celui des « données savantes » (*sapient data*). En sorte, une crypto-monnaie qui « colle » parfaitement à son possesseur et à ses valeurs.

À méditer.

Les Colored Coins (variante de bitcoins)

Le principe des Colored Coins[1] est de « colorier » certains des bitcoins en circulation et de leur assigner des propriétés spécifiques, dont la valeur peut être différente du sous-jacent bitcoin.

Colored Coins est un protocole bitcoin 2.0 en *open source* et le système est séparé en deux niveaux :

- le système Bitcoin tel que nous le connaissons ;
- un réseau dépendant du protocole Bitcoin mais autonome.

Cette dissociation permet d'émettre des instruments d'échange distincts du réseau Bitcoin. Il s'agit d'un « protocole dans le protocole », pouvant être utilisé comme une monnaie alternative, des produits dérivés, des actions ou obligations, voire de la propriété intelligente, tout en utilisant l'infrastructure et le réseau Bitcoin.

On pourrait très bien imaginer la création d'un fonds de sécurité sociale indépendant et décentralisé à partir de ces Colored Coins, et géré par la communauté qui y souscrit.

1. http://coloredcoins.org/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Counterparty[1] (variante de bitcoin)

Counterparty est une plateforme et un portefeuille construits par-dessus la blockchain du bitcoin et qui permet de créer des avoirs par tokenisation[2]. Counterparty a sa propre monnaie qui s'appelle XCP. La monnaie est utilisée pour échanger des biens et aussi pour créer des contrats intelligents qui tournent sur la plateforme moyennant des honoraires en XCP. Ces avoirs sont divisibles et programmables et peuvent être envoyés d'une adresse à une autre pendant l'exécution des *smart contracts*. En gros, Counterparty est l'équivalent de la plateforme Ethereum mais en utilisant la blockchain Bitcoin.

Augmentation de la taille des blocs de transactions

Actuellement, le réseau Bitcoin traite environ 160 000 transactions par jour et les blocs sont, en moyenne, remplis à 50 %, soit 0,5 Mo. Les pics d'activité sont donc assez rapidement absorbés, et toutes les transactions, même sans frais, finissent par être validées. Cependant, si Bitcoin poursuit sa progression au rythme actuel, il se pourrait bien que la limite de 1 Mo soit atteinte l'année prochaine. Dès lors, les utilisateurs seront mis en concurrence sur les frais qu'ils daignent verser aux mineurs et les transactions n'incluant pas ou peu de frais ne seront plus validées.

Le problème est que, dans ce scénario, le réseau Bitcoin finirait par ne traiter que les transactions importantes à frais élevés (en valeur absolue, mais faibles en proportion du montant) et pourrait par exemple évoluer en réseau de compensation entre sociétés.

Alors comment limiter le risque d'une plus grande centralisation et donc d'un affaiblissement du réseau ?

1. https://counterparty.io/
2. Voir glossaire : http://www.blockchaindailynews.com/glossary/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

L'analyse de Pierre Noizat

Pierre Noizat[1] nous apporte son éclairage sur le point souvent débattu de l'augmentation de la taille des blocs : « C'est une solution pratique et relativement simple à déployer, déjà préconisée par Gavin Andresen[2]. Elle s'accompagne bien sûr d'un alourdissement de la blockchain qui peut être géré grâce aux checkpoints. Un checkpoint est un numéro de bloc codé "en dur" dans le *wallet* qui est considéré comme sûr par les mineurs pour reconstituer l'historique complet des transactions.

Le consensus s'établit sur le fait que les transactions antérieures à ce bloc, par exemple des transactions confirmées il y a plus de deux ans, ne peuvent plus être invalidées par une réorganisation de la blockchain résultant d'une attaque des 51 %. »

En revanche, entre la volonté d'augmenter la taille des blocs et le passage à l'acte il y a un fossé difficile à combler. En effet, les « sages » de la blockchain Bitcoin ne font pas toujours consensus quand il s'agit de réviser le code du protocole[3]… Ce qui fait que ce problème demeure en suspens.

Les sidechains ou chaînes collatérales

Les altcoins ne posent-ils pas des problèmes de vulnérabilité, de pérennité ? Le débat reste ouvert mais des questions fondamentales demeurent posées à propos de la blockchain Bitcoin.

En réalité, le problème technique majeur est celui de l'interopérabilité avec les systèmes existants et potentiellement entre les différents réseaux de blockchains. Comment ces *ledgers* pourront interagir s'ils sont construits séparément pour

1. Pierre Noizat : http://e-ducat.fr
2. Gavin Andresen est le scientifique en chef de la Fondation Bitcoin. Il possède une clé cryptographique qui lui permet de publier une alerte à tous les clients Bitcoin. Son site perso : http://gavinandresen.ninja/
3. https://bitcoin.fr/quel-est-lenjeu-du-debat-sur-la-taille-minimale-des-blocs-de-transactions/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

différents types d'actifs et fonctionnent avec la technologie de l'infrastructure du marché existant ?

C'est ce qu'Adam Back[1], inventeur de HashCash[2] (*proof of work algorithm*[3]) et cofondateur de Blockstream[4] a constaté à propos de la blockchain Bitcoin.

En effet, il pense que l'évolution de la blockchain Bitcoin ne peut se faire que très lentement à cause des décisions autour de son évolution qui se font selon un processus qui exige un accord difficile à obtenir de la part de ceux qui travaillent à le surveiller et qui ne sont pas organisés en structure hiérarchique. C'est d'ailleurs un problème récurrent avec les applications totalement décentralisées dont, par nature, le contrôle n'est entre les mains de personne.

Sur ce constat, et avec une équipe de chercheurs, Adam Back a mis au point une méthode liant les blockchains les unes aux autres, le système « *sidechain*[5] », pour lequel un livre blanc[6] a été publié en 2014[7].

1. Site personnel : http://www.cypherspace.org/adam/
2. 1997 : Adam Back invente HashCash, un système de preuve de travail à partir d'une idée introduite par Cynthia Dwork et Moni Naor dans un rapport publié en 1993, « Pricing *via* Processing or Combatting Junk Mail ». Adam Back deviendra plus tard le premier interlocuteur de Satoshi Nakamoto puis récemment le cofondateur de Blockstream.
3. http://www.hashcash.org/
4. https://blockstream.com
5. https://blockstream.com/technology/#sidechains
6. https://blockstream.com/technology/sidechains.pdf
7. Voir également le projet « Éléments » ou « Elementsproject » (https://elementsproject.org/sidechains/) initié par Blockstream et une communauté. Vous pouvez rejoindre ce projet et créer votre propre sidechain (https://elementsproject.org/sidechains/creating-your-own.html).

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Dans les faits, le système des sidechains[1] permettrait de faire passer des unités monétaires d'une chaîne A vers une chaîne B. Elles disparaîtraient de la chaîne A pour réapparaître sur la chaîne B et pourraient éventuellement revenir dans A.

Rootstock[2] et Interledger

Rootstock (RSK) est basé sur des concepts identiques à Ethereum (voir sous-chapitre suivant) mais sur une sidechain du réseau Bitcoin.

Le projet *open source* RSK est une plateforme de *smart contracts* de pair à pair[3]. Son objectif principal est de tirer parti de la solution de contrat intelligent que Rootstock, une start-up basée à Buenos Aires, a développé. Le consortium construira une couche Turing-complet[4], un contrat intelligent, au-dessus de bitcoin pour soutenir une large gamme d'applications. Ce projet permettra d'apporter au réseau Bitcoin des fonctionnalités similaires à Ethereum.

Le principe est qu'à chaque fois qu'une personne ou une société gère un contrat intelligent avec RSK, alors 80 % du « carburant » payé sont versés aux mineurs et les 20 % restants à RSK Labs, ce qui permet à RSK de continuer le développement de la plateforme *open source*.

1. Pour plus de détails sur le fonctionnement des sidechains, vous pouvez consulter un article de Pierre Noizat dédié aux sidechains (http://e-ducat.fr/2014-11-08-blockchain-et-sidechains/).
2. http://www.rsk.co/#1
3. Projet Rootstock sur bitcoin.fr : https://bitcoin.fr/rootstock-bitcoin-pour-les-smart-contracts/
4. Turing-complet : machine de Turing universelle qui a potentiellement la capacité de calculer tout ce qui est calculable. En informatique théorique, une machine de Turing est un modèle abstrait du fonctionnement des appareils mécaniques de calcul, tels un ordinateur et sa mémoire. Ce modèle a été imaginé par Alan Turing en 1936, en vue de donner une définition précise au concept d'algorithme ou de procédure mécanique.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Selon les concepteurs de la plateforme, RSK n'est pas un concurrent de Ethereum. Ils précisent qu'ils ont l'intention que RSK soit compatible avec les applications déjà en cours d'exécution sur Ethereum et ainsi de permettre une communication entre Bitcoin et Ethereum grâce à une fonctionnalité à deux voies (2WP) intégrée à la plateforme RSK qui permet le transfert de bitcoins vers une autre blockchain, comme par exemple Ethereum, et inversement.

Le consortium RSK (Rootstock, rhizome en français) regroupe plus de 25 grandes entreprises de l'écosystème Bitcoin, dont Consilium, Bitmain, Xapo, Jaxx, Skry, BitGo, Richfund, Bitpay, Antpool, Blocktrail, Bitex, Digital Currency Group, BTCC, Unocoin, Bitso, Bitstamp, Bitfinex, BitPay, Signatura, Wings, etc.

C'est donc un vaste projet qui ne peut qu'enrichir les fonctionnalités de Bitcoin tout en conservant ses valeurs intrinsèques.

Quant au protocole Interledger[1], développé par Ripple Labs, pour relier les blockchains aux registres distribués, il permet des paiements à travers des réseaux différents et utilise des dépôts fiduciaires pour traiter les mouvements de fonds entre deux livres séparés. Contrairement à l'approche bitcoin, ce protocole n'exige aucun système de coordination globale de blockchain.

Lightning Network[2]

La blockchain Bitcoin est très prometteuse dans le domaine des grands livres distribués, mais en tant que plateforme de paiement elle ne peut, aujourd'hui, englober les transactions du commerce mondial.

1. https://interledger.org/
2. https://lightning.network/. Voir aussi : https://bitcoin.fr/lightning-network-la-solution-pour-bitcoin/ et http://blogchaincafe.com/the-lightining-network-pour-un-reseau-bitcoin-totalement-scalable

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Ainsi ses qualités sont aussi des freins à son expansion. En effet, toutes les modifications au sein du grand livre étant diffusées à l'ensemble des nœuds (participants), cela signifie que chaque nœud du réseau Bitcoin connaîtrait toutes les transactions qui se produisent à l'échelle mondiale, ce qui créerait automatiquement un énorme frein sur les temps de réponse du réseau.

D'où l'idée de créer un système parallèle englobant toutes les transactions de manière à ne pas sacrifier la décentralisation et la sécurité que fournit le réseau Bitcoin.

Ce nouveau système de micropaiement sur Bitcoin à l'initiative de Blockstream qui collabore avec les leaders de l'industrie est le Lightning Network. Il prendrait en charge de grands volumes de micropaiements (la mise en place de cette solution ferait passer la limite du nombre de transactions par seconde de 7 à plus de 7 000) en utilisant des frais de transaction quasi nuls et en fonctionnant à la vitesse de « l'éclair ». Un premier « draft » est paru en février 2015 et un livre blanc a été publié en janvier 2016[1].

À ce jour, il existe quatre implémentations de Lightning (source Bitcoin.fr) :

- Lightning Corp (auteurs originaux) et Bitfury[2] (pas d'implémentation propre mais une collaboration avec LN Corp. sur le routing) ;
- Blockstream ;
- Blockchain.info ;
- Éclair d'ACINQ[3].

1. https://lightning.network/lightning-network-paper.pdf
2. http://bitfury.com/
3. http://acinq.co/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

L'analyse de Pierre-Marie Padiou cofondateur d'ACINQ

En septembre 2016, ACINQ, start-up française, annonçait avoir mis en œuvre avec succès l'algorithme de routage Flare de Bitfury dans Éclair (solution ACINQ), et l'avoir testé sur un réseau de 2 500 serveurs. C'est une première étape prometteuse dans le développement d'un cadre de routage évolutif pour le réseau Lightning.

« Éclair est notre implémentation du réseau Lightning, qui vise à résoudre un certain nombre de limitations de Bitcoin. Ces limitations avaient été assez largement évoquées lors du fameux débat sur la taille des blocs : il s'agit principalement de la capacité du réseau à traiter un flux important de transactions (actuellement < 10 tx/s).

Pour nous, c'est une avancée essentielle qui permettra de désaturer le réseau Bitcoin et de passer à l'échelon supérieur, en termes de performance, et de cas d'utilisation, avec des transactions instantanées et très peu coûteuses. C'est un peu difficile d'en dire plus à ce stade car nous n'avons pas encore de produit "grand public" à présenter et le sujet est technique. Il y a plusieurs efforts d'implémentation menés en parallèle par différentes sociétés (Blockstream, Lightning Corp, Blockchain.com et nous), et l'heure est actuellement à la convergence vers une solution interopérable, ce qui est une très bonne chose[1]. »

Si la communauté Bitcoin fait « consensus », alors 2017 devrait être l'année de l'aboutissement pour le réseau Lightning.

1. Interview ACINQ : http://www.blockchaindailynews.com/Blockchain-Bitcoin-Eclair-et-reseau-Lightning_a24530.html

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Le livre blanc de Bitfury[1]

Ce livre blanc, « Flare : An Approach to Routing in Lightning Network » (juillet 2016), traite de Flare, un algorithme de routage hybride pour l'acheminement des paiements sur le Lightning Network.

Il suggère un algorithme en deux phases :

- une mise à jour proactive de la carte de routage du nœud, qui stocke des informations sur la topologie du réseau ;
- la collecte réactive d'informations selon les besoins lorsqu'une requête Lightning Network le demande.

Ce livre blanc est la première tentative de décrire et de tester préliminairement une solution algorithmique pour la future implémentation du Lightning Network sur la blockchain Bitcoin qui permettra une évolutivité du traitement des transactions.

Les « side databases » ou blockchain databases

Au même titre que les sidechains existantes ont été créées pour améliorer les temps de réponse des blockchains historiques, il existe désormais des bases de données qui permettent de booster les transferts et le traitement des données : nous les appellerons, par ce néologisme, les « side databases ».

Dans les faits, si l'on mesure les performances de la blockchain Bitcoin avec les critères des bases de données traditionnelles, nous avons un retour catastrophique :

1. « Flare : An Approach to Routing in Lightning Network » (fruit de la collaboration entre le coauteur Olaoluwa Osuntokun et le reste de l'équipe du réseau Lightning), http://bitfury.com/content/5-white-papers-research/whitepaper_flare_an_approach_to_routing_in_lightning_network_7_7_2016.pdf

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

- le *throughput*[1] (débit) est de seulement quelques transactions par seconde (tps) ;
- le délai avant qu'une opération d'écriture ne se réalise est de dix minutes ;
- la capacité est de l'ordre de quelques douzaines de gigabytes (GB)[2] ;
- il n'y a pas de scalabilité linéaire lors de l'ajout de nœuds : avec un doublement de nœuds, le trafic du réseau quadruple sans aucune amélioration du *throughput*, de la latence ou de la capacité ;
- l'ajout de nœuds se fait correctement jusqu'à environ 10 000, puis la performance chute ;
- il n'y a pas la possibilité de faire des *query* (requêtes) sur les données, avec ou sans SQL.

Pour améliorer ces performances, il semble que BigchainDB[3] ait trouvé la solution.

BigchainDB est une base de données scalable, compatible avec Bitcoin, Ethereum, Chain, Eris, etc. et comble un vide en se positionnant comme un pont entre la blockchain et le système de stockage.

Mais même en laissant de côté l'aspect blockchain, BigchainDB offre beaucoup de fonctionnalités manquant au NoSQL et aux bases de données distribuées. Ce seul fait est déjà une bonne raison de l'adopter dans de nombreux cas d'usage qui étaient jusqu'ici encombrés par les limitations de scalabilité des bases

1. Voir glossaire : http://www.blockchaindailynews.com/glossary/
2. Unité de mesure de stockage en informatique équivalent à un milliard de bytes.
3. https://www.bigchaindb.com

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

de données blockchain. De plus, le système de personnalisation permet des configurations qui s'adaptent aux blockchains privées et publiques.

Ascribe[1]

Ascribe est une start-up allemande qui utilise la blockchain Bitcoin pour enregistrer une quantité limitée d'ID uniques aux œuvres numériques, ce qui les rend traçables et leur donne plus de valeur, en raison de cette quantité finie de copies.

Ascribe, qui a rencontré de nombreux problèmes technologiques principalement en raison des limitations de la blockchain Bitcoin, décide ainsi de combiner le meilleur des deux mondes, en prenant une base de données NoSQL, RethinkDB[2], et en y ajoutant une couche blockchain pour ajouter le contrôle décentralisé, la création et le mouvement d'actifs numériques, le suivi de ces actifs, l'immutabilité et un niveau de sécurité supplémentaire. Du sur mesure en quelque sorte.

Refermons ici cette revue des solutions nouvelles qui viennent compenser ou booster les quelques lacunes des blockchains historiques.

La technologie progresse très vite et dans quelques jours ou semaines, nous verrons poindre de nouvelles fonctionnalités et de nouvelles possibilités. Le monde des blockchains n'a pas fini sa mue et les évolutions vont se suivre à un rythme soutenu.

1. https://www.ascribe.io/
2. https://www.rethinkdb.com/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Blockchain Ethereum

Impossible de parler de la blockchain sans aborder Ethereum qui est souvent présenté par rapport à Bitcoin comme le Bitcoin 2.0, le prochain Bitcoin, ou encore « Bitcoin on Steroids[1] ».

Un peu d'histoire

Vitalik Buterin[2] est le créateur d'Ethereum. Il a d'abord découvert les technologies blockchain et les crypto-monnaies à travers Bitcoin en 2011, et a été immédiatement emballé par la technologie et son potentiel. Il a cofondé *Bitcoin Magazine* en septembre 2011 et, après deux ans et demi de réflexion sur la technologie et les applications existantes, il publie son idée sous la forme d'un livre blanc[3] en novembre 2013.

Vitalik Buterin pense que la blockchain, technologie sous-jacente au Bitcoin, devrait faire plus que de simplement déplacer de l'argent d'un point A à un point B. D'après lui, Satoshi Nakamoto avait uniquement conçu la blockchain Bitcoin pour réaliser des transactions monétaires et, même avec des ajustements, cette blockchain ne pouvait rien délivrer d'autre.

Vitalik Buterin écrit que la blockchain Bitcoin a été conçue pour être un protocole SMTP (Simple Mail Transfer Protocol). C'est un protocole excellent pour une tâche particulière, le transfert d'argent, mais il n'a pas été pensé en tant que couche fondamentale sur laquelle on pourrait bâtir tout type de protocoles.

1. Source : http://www.bortzmeyer.org/ethereum.html
2. https://about.me/vitalik_buterin
3. Livre Blanc / White Paper Ethereum – Traduction française : https://www.ethereum-france.com/livre-blanc-white-paper-ethereum-traduction-francaise/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

À partir de ces constats, Vitalik Buterin entreprend de créer une blockchain différente qui pourrait supporter un nombre illimité d'applications. Ethereum est né.

Début 2014, il met en prévente les premiers ethers[1] afin d'obtenir les fonds nécessaires au développement du projet (il obtient ainsi près de 18 millions de dollars). Le 30 juillet 2015, Frontier, la première version d'Ethereum, est publiée et le bloc genesis[2] est créé.

Vitalik Buterin dirige maintenant l'équipe de recherche d'Ethereum qui travaille sur les futures versions du protocole Ethereum.

L'analyse de Vitalik Buterin

Dans son livre blanc, Vitalik Buterin nous propose sa définition : « Le but d'Ethereum est de créer un protocole alternatif pour construire des applications décentralisées, fournissant un ensemble différent de compromis que nous pensons être très utile pour une vaste classe d'applications décentralisées, avec un accent particulier sur les situations où le développement rapide, la sécurité des petites applications rarement utilisées et la possibilité pour les différentes applications d'interagir ensemble de manière très efficace sont importants. Ethereum fait cela en construisant ce qui est essentiellement la couche fondamentale abstraite ultime : une blockchain intégrant un langage de programmation Turing-complet, permettant à quiconque de rédiger des *smart contracts* (contrats autonomes) et des applications décentralisées où l'on peut créer ses propres règles concernant la propriété, les formats de transaction et les fonctions de transition d'état. Une version dépouillée de Namecoin peut être écrite en deux lignes de code et d'autres protocoles comme les devises et les systèmes de réputation peuvent être développés en moins de vingt lignes. »

1. Ether : monnaie de la blockchain Ethereum.
2. Bloc genesis : la genèse d'une blockchain, c'est-à-dire le premier bloc d'une blockchain.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Chronologie des versions

2013

- Novembre : publication du livre blanc.

2014

- 1er février : Proof of Concept (PoC) 1 ;
- 20 février : PoC 2 ;
- 1er mars : PoC 3 ;
- 9 avril : PoC 5 ;
- 22 juillet au 2 septembre : vente ethers ;
- 5 octobre : PoC 6.

2015

- 13 janvier : PoC 7 ;
- 24 février : PoC 8 ;
- 9 mai : Olympic ;
- 30 juillet : Frontier.

2016

- 13 février : 1 000 000 Blocks ;
- 14 mars : Homestead ;
- Projet : Metropolis ;
- Projet : Serenity ;
- Projet : Ethereum 2.0 ;
- Projet : Ethereum 3.0.

Vous trouverez plus de détails concernant les étapes du lancement d'Ethereum sur le site d'Ethereum France et sur celui de Blogchain Café[1].

1. Étapes du lancement d'Ethereum sur Ethereum France : https://www.ethereum-france.com/etapes-du-lancement-dethereum/ ; sur Blogchain Café : http://blogchaincafe.com/les-differentes-etapes-du-lancement-dethereum

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Définition

À l'instar de la blockchain Bitcoin, Ethereum est une blockchain publique dont la particularité est de permettre la création par les utilisateurs de contrats intelligents, grâce à un langage Turing-complet[1], contrats qui sont basés sur un protocole informatique permettant de vérifier ou de mettre en application un contrat mutuel, et qui sont déployés et consultables publiquement dans la blockchain.

L'analyse d'Ethereum.org[2]

Voici comment Ethereum.org présente le principe : « Ethereum est une plateforme décentralisée qui exécute des contrats intelligents, c'est-à-dire des applications programmées qui fonctionnent sans aucune possibilité d'arrêt, de censure, de fraude ou d'interférence de la part d'un tiers.

Ces applications s'exécutent sur une blockchain personnalisée, une infrastructure mondiale partagée. Cela permet aux développeurs de créer des marchés, de stocker des registres de dettes ou de promesses, de déplacer des fonds conformément aux instructions données préalablement (comme une volonté ou un contrat à terme) et beaucoup d'autres choses qui n'ont pas encore été inventées, ou le risque de contrepartie.

Le projet a été amorcé par une prévente d'ethers en août 2014 par des fans du monde entier. Il est développé par la Fondation Ethereum[3], un organisme suisse sans but lucratif, avec des contributions de grands esprits à travers le monde. »

1. En informatique ou en logique, un système Turing-complet est un système formel ayant une puissance de calcul au moins équivalente à celle des machines de Turing. Voir glossaire : http://www.blockchaindailynews.com/glossary/
2. https://www.ethereum.org/
3. Ethereum Foundation : https://ethereum.org/foundation

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Le minage

À l'instar du protocole Bitcoin, Ethereum fait appel au minage *proof of work*. Toutefois, le protocole Ethereum prévoit de basculer prochainement du minage *proof of work* actuel (Frontier) à un minage *proof of stake*[1] (Casper[2] : algorithme non finalisé en date du 6 septembre 2016).

La monnaie

Ethereum utilise une unité de compte dénommée ether comme moyen de paiement des contrats. Le sigle correspondant, utilisé par les plateformes d'échange, est ETH. L'ether est la deuxième plus importante monnaie cryptographique décentralisée, après le bitcoin, avec une capitalisation supérieure à 1 milliard d'euros[3].

L'achat d'ethers

Pour acheter des ethers[4], il y a deux solutions :

- acheter des ethers par carte bleue *via* une plateforme (voir la liste en fin d'ouvrage) ;
- échanger des ethers contre des bitcoins ou une autre crypto-monnaie.

La première solution est plus rapide, mais plus chère. Il faut passer par une plateforme (Coinhouse[5] par exemple), qui vous permet d'acheter directement des ethers. Normalement,

1. Voir glossaire : http://www.blockchaindailynews.com/glossary/
2. The Mauve Revolution : https://www.ethereum-france.com/%EF%BB%BFethereum-2-0-mauve-paper-traduction-francaise/
3. Voir CoinMarketCap : http://coinmarketcap.com/#EUR
4. Pour obtenir les informations complètes sur les deux solutions, rendez-vous sur https://www.ethereum-france.com/comment-acheter-des-ethers-eth/
5. https://www.coinhouse.io/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

quelques heures suffisent pour la création d'un compte, la vérification de l'identité et pour effectuer des transactions. En revanche, une commission de 6 à 10 % s'applique.

La seconde solution est plus longue, mais moins coûteuse. Il faut se rendre sur une plateforme d'échange, comme Kraken, puis effectuer un virement depuis son compte bancaire vers cette plateforme pour acheter des bitcoins, et ensuite échanger ses bitcoins contre des ethers.

Fonctionnement

On peut considérer Ethereum comme un ordinateur mondial (constitué de milliers d'ordinateurs) à travers le monde, auquel tout le monde peut accéder. Sa puissance de calcul provient des mineurs, qui sont rétribués en « gaz ».

Les mineurs exécutent collectivement les opérations nécessaires (vérification, ajout de données, exécution de *smart contracts*) au fonctionnement de la blockchain Ethereum en échange de cette rétribution. Le gaz peut être échangé contre des ethers, qui eux-mêmes peuvent être échangés contre des monnaies fiat sur les plateformes de marchés.

On peut donc stocker ce que l'on souhaite sur la blockchain Ethereum, même du code. Cette blockchain est à disposition des particuliers comme des professionnels, qui peuvent s'en servir librement.

Ethereum se distingue des autres blockchains par les *smart contracts* (contrats intelligents) et les DAO (*decentralized autonomous organizations*, organisations autonomes décentralisées).

Ce système permet la réduction du nombre de contentieux ainsi qu'une gestion plus aisée de ceux-ci. Dans ce système, il

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

n'est pas besoin de faire confiance au partenaire, ni à une autorité centrale. C'est le système informatique totalement automatisé qui garantit l'honnêteté de la transaction.

Smart contracts, DAO

Les *smart contracts*

Nick Szabo, spécialiste du chiffrement, créateur d'un réseau précurseur de Bitcoin, appelé BitGold, et d'ailleurs soupçonné d'être le mystérieux inventeur de Bitcoin, a développé l'expression et le concept de *smart contracts*[1] en 1994. En réalité, il souhaitait associer d'une façon automatique des contrats intelligents à des transactions dans le domaine du commerce électronique entre des personnes qui ne se connaissent pas sur Internet[2].

Les *smart contracts* sont des programmes informatiques qui enregistrent et/ou exécutent les termes d'un contrat lorsque les échéances arrivent à terme (un prêt financier, l'émission d'une action, un vote, un contrat de mariage, tout type de contrat…) dont les caractéristiques ont été au préalable clairement définies[3].

L'objectif est de satisfaire les conditions contractuelles, comme les termes du paiement, de la livraison, mais aussi de la confidentialité, et même de l'exécution des obligations réciproques. Le caractère numérique et automatisé du contrat permet donc

1. *Smart contracts* par Szabo : http://www.virtualschool.edu/mon/Economics/SmartContracts.html et http://szabo.best.vwh.net/smart_contracts_idea.html
2. « Bitcoin is not just digital currency. It's Napster for finance », *Fortune*, janvier 2014.
3. Voir S. Bourque et S. Fung Ling Tsui, « A Lawyer's Introduction to Smart Contracts », *Scientia Nobilitat Reviewed Legal Studies*, 2014.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

en théorie à deux partenaires de nouer une relation commerciale sans qu'ils aient besoin de se faire confiance au préalable, sans autorité ou intervention centrale. C'est en effet le système lui-même, et non ses agents, qui garantit l'honnêteté de la transaction. Tel est le sens du projet Ethereum[1] qui permet la création de *smart contracts* à grande échelle[2] en mettant en place une méthode de vérification entièrement dématérialisée qui peut être effectuée directement par les pairs sans l'interférence d'outils juridiques.

Dans la blockchain, ce sont des programmes accessibles et consultables par toutes les parties autorisées et dont l'exécution est contrôlée et vérifiable. Ces programmes exécutent de façon automatique les conditions d'un contrat lorsque certains éléments sont réunis.

Ces contrats « intelligents » permettent de donner une dimension intelligente à la blockchain : dans le cadre d'un contrat d'assurance, si les conditions de remboursement sont réunies, alors le contrat s'exécute et opère une transaction pour indemniser l'assuré. Grâce aux *smart contracts*, la blockchain ne se limite plus au stockage de l'information !

Les contrats intelligents permettent d'enregistrer de manière sécurisée les informations contractuelles reliant les parties entre eux. Les termes du contrat, les informations sur les différentes parties et les dates sont conservés. La blockchain permet ici d'avoir une preuve datée digitale irréfutable et infalsifiable.

1. Pour une explication technique du projet, voir http://www.bortzmeyer.org/ethereum.html
2. Comme tout système de registre décentralisé, la vérification coûte cher et les pairs doivent être incités à travailler ; d'où le développement des jetons (« token ») ou des points spécifiques à Ethereum, l'ether : il n'y a donc pas de mineurs contrairement au système Bitcoin dans lequel les mineurs sont rémunérés par des bitcoins.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Il est important de relever que les *smart contracts* sont à double tranchant. En effet, si l'immuabilité peut être souhaitable, en cas d'erreur dans l'écriture du code du contrat, il sera impossible de revenir en arrière.

Sur Ethereum, chaque *smart contract* est inscrit dans un bloc de la chaîne à l'aide d'un langage dédié, Solidity[1]. Solidity est un langage de haut niveau, dont la syntaxe est similaire au JavaScript. Il a été conçu pour permettre de compiler du code pour les machines virtuelles d'Ethereum[2]. Langage Turing-complet, Solidity permet d'écrire des programmes simples comme complexes[3].

Aujourd'hui, on peut trouver sur Ethereum des contrats (distribution, royalties, pactes d'actionnaires…) mais aussi des projets plus complexes (crypto-monnaie, plateforme de financement décentralisée, DAO…).

Pour un contrat intelligent dont les conditions d'exécution sont liées à des indicateurs temporels ou à des écritures dans la blockchain, la vérification est automatique. En revanche, dans le cas où il faut vérifier une condition externe (que le colis a bien été reçu), il faut faire appel à un tiers de confiance, un Oracle[4]

1. https://solidity.readthedocs.io/en/develop/ et https://github.com/ethereum/wiki/wiki/The-Solidity-Programming-Language
2. Le code utilisé dans le projet Ethereum est différent de celui utilisé par le Bitcoin, même s'il s'en inspire. Le code a été réécrit à partir de zéro. La principale différence par rapport à Bitcoin est que les transactions stockées dans la blockchain ne sont pas limitées à envoyer et recevoir de l'argent. Ethereum dispose d'un quasi-langage de Turing et est donc un système de calcul réparti : les pairs dans le réseau Ethereum ne se contentent pas de vérifier l'intégrité de la blockchain et d'ajouter de la monnaie, ils exécutent du code arbitraire, celui des applications que vous ou moi développons et envoyons sur le réseau.
3. Pour en savoir plus sur la programmation de *smart contracts*, voici un lien pédagogique : http://blogchaincafe.com/la-programmation-de-smart-contract-une-operation-hautement-delicate
4. Voir glossaire : http://www.blockchaindailynews.com/glossary/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

dans le jargon d'Ethereum. L'Oracle peut être un tiers désigné par les deux parties, un institut/association de confiance ou encore un consensus de nombreux tiers (projet Oraclize[1]).

L'Oracle par Ethereum France

« L'Oracle a écrit à minuit, le 8 juillet 2016 à l'adresse 0x3615087316813abba..., que la France a gagné 2-0 contre l'Allemagne à l'Euro. Lors de son exécution le 9 juillet, le *smart contract* de pari qui fait appel à cette information en déduit que le parieur A a perdu car il avait envoyé une transaction pariant sur l'Allemagne, alors que B, qui avait envoyé une transaction pariant sur la France, a gagné et doit récupérer ses gains, qui lui sont automatiquement envoyés[2]. »

L'exécution du contrat nécessite le « gaz » (d'une valeur de l'ordre du centime d'euro pour un contrat simple à quelques euros pour un contrat complexe).

Dans ce vaste domaine des contrats intelligents, tout l'enjeu consiste à savoir comment lier un contrat fiat (qui a trait à l'environnement juridique) et un contrat encrypté dans la blockchain.

Codius[3] et les contrats intelligents

Codius est un projet Ripple Labs, actuellement en version bêta et *open source*. Ainsi lorsque deux personnes effectuent des transactions, elles peuvent écrire les termes de leurs transactions en code, mais aucune d'elles ne peut faire

1. http://www.oraclize.it/
2. Oracle – Ethereum France : https://www.ethereum-france.com/les-oracles-lien-entre-la-blockchain-et-le-monde/
3. https://www.codius.org/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

confiance à l'autre pour l'exécuter. C'est ici que Codius intervient en permettant à un tiers de l'exécuter et d'attester de l'intégrité du code exact qu'il a reçu.

Nous sommes ici en présence d'un développement dédié à l'origine au monde de la finance et qui est utilisable en langage web.

DAO (*decentralized autonomous organization*)

Principe

DAO[1] est l'acronyme de *decentralized autonomous organization* ou, en français, organisation autonome décentralisée[2]. Comme son nom l'indique, c'est une organisation autonome (sans organe central de contrôle) qui fonctionne grâce à un ou des contrats intelligents qui apportent à une communauté des règles transparentes et immuables de gouvernance et des échanges sécurisés.

C'est ce que l'on nomme parfois un système de gouvernance 2.0 (exemple Bitnation[3]) ou de gouvernance participative.

L'analyse de Vitalik Buterin[4]

« On peut facilement faire un contrat de produits dérivés financiers, mais en utilisant un flux de données météo au lieu d'un indice de prix. Si un agriculteur dans l'Iowa achète un dérivé dont les

1. https://www.ethereum-france.com/decentralized-autonomous-organization-dao-blockchain/ et « Qu'est-ce qu'une DAO ? », https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/
2. Pour en savoir plus sur la DAO, reportez-vous à l'article « DAO : Contractors et Curators », http://blogchaincafe.com/dao-contractors-et-curators
3. https://bitnation.co/
4. Assurance récolte : https://www.ethereum-france.com/livre-blanc-white-paper-ethereum-traduction-francaise/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

paiements sont inversement proportionnels aux précipitations dans l'Iowa et qu'une sécheresse se produit, l'agriculteur recevra automatiquement de l'argent. S'il y a suffisamment de pluie, l'agriculteur sera satisfait car ses cultures se porteront bien. Cela peut être étendu aux assurances contre les catastrophes naturelles en général. »

Notons que si les DAO baignent actuellement dans le vide juridique, une législation les concernant devrait émerger dans un avenir proche. En effet, dans l'état actuel des choses, les DAO sont vulnérables à certaines situations. Par exemple, si une DAO confie ses fonds à un prestataire qui n'honore pas le contrat (pas assez de mécanisme de contrôle dans le *smart contract* reliant DAO et prestataire), elle ne peut pas se retourner contre lui juridiquement. Elle n'a aucune existence juridique, et à ce titre le contrat entre la DAO et le prestataire n'a aucune valeur.

Cela n'est qu'un exemple des limites de la DAO. Cette nouvelle forme d'organisation est encore récente, et elle sera amenée à évoluer pour en permettre une utilisation optimale.

L'analyse de maître Thibault Verbiest[1]

« Une DAO est une organisation fonctionnant grâce à un programme informatique qui fournit des règles de gouvernance à une communauté d'utilisateurs. C'est une version plus complexe d'un *smart contract*, avec les mêmes avantages que celui-ci : ses règles sont transparentes et immuables car inscrites dans la blockchain.

Ces organisations autonomes décentralisées, par nature horizontales, présentent un potentiel de rupture majeur par rapport aux modes d'organisations classiques hérités de la révolution industrielle, basés sur une logique verticale, avec au sommet des actionnaires cherchant un réaliser un profit.

1. « Les organisations distribuées autonomes : quel statut juridique ? », maître Thibault Verbiest, avocat associé du cabinet De Gaulle Fleurance & Associés.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Ces DAO vont-elles tenir leur promesse d'un monde économique plus libre, transparent et démocratique au sens premier du terme ?

Pour ce faire, elles devront passer le test de la gouvernance, comme n'importe quelle organisation humaine. Et, à court terme, se posera aussi la question de leur place dans l'ordre étatique traditionnel. Comment pourront-elles interagir avec d'autres sujets de droit (créanciers, débiteurs, régulateurs, etc.) ?

The DAO sur Ethereum

La première expérience en la matière est The DAO, sur la blockchain Ethereum, qui a récemment défrayé la chronique.

The DAO est une sorte de fonds d'investissement décentralisé dont la fonction est triple : évaluer des projets qui lui sont soumis ; décider collectivement avec les détenteurs de jetons de la DAO de financer ou non ces projets ; distribuer les risques et récompenses qui y sont relatifs.

Dans cette DAO, il y a d'une part des détenteurs de jetons qui constituent les « actionnaires » de la DAO, et d'autre part des prestataires.

Les premiers participent à la création de la DAO, investissent de l'argent en échange de jetons, et constituent la base de la DAO.

Les seconds sont ceux qui soumettront des projets à la DAO et demanderont du financement.

Le projet The DAO implique également des curateurs, qui filtrent les projets, en vérifiant que le code source fourni par un prestataire correspond bien à ce qu'il propose. Leur travail est auditable par chacun, et s'ils sont "corrompus", ils peuvent être écartés.

Autre exemple de DAO : une communauté s'auto-assure contre la perte d'emplois, sans passer par une compagnie d'assurances ou un courtier. Elle crée une cagnotte (en bitcoins ou en ethers par exemple) et lorsque l'un de ses membres perd son emploi (l'information étant transmise, *via* un API, par l'autorité habilitée à constater la perte d'emploi), une somme préalablement convenue lui est payée. Tout est exécuté par un *smart contract*.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

L'absence de personnalité juridique

À première vue, la DAO, en tant que telle, ne peut signer de contrat avec une autre entreprise, ouvrir un compte en banque, agir ou être attraite en justice.

Toutefois, il est probable qu'un juge considérera qu'une DAO constitue une société créée de fait. Une telle constatation résulte du comportement de personnes qui, sans en avoir pleinement conscience, se traitent entre elles et agissent à l'égard des tiers comme de véritables associés.

La société créée de fait est soumise au même régime que celui de la société en participation (art. 1873 du Code civil). Selon l'article 1871 du Code civil, les rapports entre associés sont alors régis soit par les dispositions applicables aux sociétés civiles, si la société a un caractère civil, soit, si elle a un caractère commercial, par celles applicables aux sociétés en nom collectif.

Dans la pratique, les DAO auront plutôt un caractère civil (mais les usages évoluent).

Quel que soit son caractère, civil ou commercial, si la DAO ne peut pas faire face à ses dettes, ses créanciers pourront poursuivre directement les « associés » sur leurs biens personnels (à condition qu'ils soient identifiables bien entendu).

Une DAO pourrait donc exister juridiquement en tant que société en participation, mais sans personnalité juridique, ce qui n'est avantageux pour personne (sauf pour ceux qui voudraient rester anonymes...).

La pratique a déjà apporté des réponses, créatives, à cette problématique.

Ainsi, une société de droit suisse (DAO.link) s'est créée dans le but de faire le lien entre la DAO et le système juridique « traditionnel ».

À la demande du contractant de la DAO, la société DAO.link lui fournit une adresse sur la blockchain Ethereum. Cette adresse représente le contractant sur la blockchain, et le *smart contract* est conclu avec cette adresse. Dans le même temps, le contractant signe un contrat « réel », qui est le miroir du *smart contract,* avec la société suisse.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Cette dernière va donc représenter la DAO dans ses relations juridiques avec le contractant[1].

Le risque est donc déplacé sur la société DAO.link.

Une autre solution est présentée par Otonomos.com, qui crée des sociétés « miroirs » de la DAO. Les membres de la DAO sont également actionnaires de sociétés "off-shore" (pour des raisons fiscales, mais aussi pour leur souplesse en termes d'actionnariat). Inutile de dire que cette solution passera difficilement dans nos contrées...

Et la fiducie ?

Les DAO ont aussi des airs (fortuits) de parenté avec la fiducie (notre "trust" en droit civil), définie à l'article 2011 du Code civil : "La fiducie est l'opération par laquelle un ou plusieurs constituants transfèrent des biens, des droits ou des sûretés, ou un ensemble de biens, de droits ou de sûretés, présents ou futurs, à un ou plusieurs fiduciaires qui, les tenant séparés de leur patrimoine propre, agissent dans un but déterminé au profit d'un ou plusieurs bénéficiaires."

Dans cette institution juridique, il n'y a pas création d'une personnalité morale, mais les biens transférés forment néanmoins un patrimoine séparé, distinct du patrimoine personnel du fiduciaire.

En outre, les "constituants" de la fiducie peuvent se désigner eux-mêmes comme "bénéficiaires".

À première vue, dans son principe, ce mécanisme semble adapté aux DAO : une communauté (les constituants) se forme pour affecter (à leur profit) des biens ou des droits (des bitcoins, des ethers, des tokens...) à un but déterminé, après avoir désigné des "curateurs" (les fiduciaires).

En pratique, est-ce réalisable ?

La fiducie requiert un contrat écrit (contenant certaines mentions obligatoires) et enregistré au service des impôts. Le contrat doit également être déclaré au registre national des fiducies.

1. https://www.ethereum-france.com/dao-link-permet-a-des-entreprises-de-contracter-avec-des-dao/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Le fiduciaire, quant à lui, doit être une institution financière ou un avocat.

Il serait donc possible de créer une DAO avec des membres qui demeurent "anonymes" sur la blockchain (identifiés uniquement par leur adresse, soit leur clé publique), mais dont l'identité serait connue des services de l'État habilités à consulter le fichier national des fiducies (juge d'instruction, etc.).

Le contrat de fiducie serait, dans toute la mesure du possible, exécutable par un *smart contract*.

Et les avocats trouveraient une fonction inattendue, celle d'"administrateurs" de DAO...

La pratique nous dira si cette approche est réaliste. »

L'attaque de The DAO ou les failles du système

Rappelons les faits : The DAO, projet lancé par une communauté organisée notamment autour de la start-up Slock.it, a démarré le 16 mai 2016 une vaste campagne de *crowdfunding* et réussi à lever plus de 120 millions de dollars en environ quatre semaines.

Le 17 juin 2016, comme le détaille Blockchain France[1], The DAO a été victime d'une attaque de grande ampleur, qui a conduit à l'arrêt de son développement.

C'est une faille présente dans The DAO qui a permis à un hacker[2] (pirate) de détourner, sur une adresse non contrôlée par les membres, un tiers des capitaux de la DAO, soit plus de 10 % du montant total de la crypto-monnaie (ether) en circulation.

1. « Qu'est-ce qu'une DAO ? » : https://blockchainfrance.net/2016/05/12/qu-est-ce-qu-une-dao/
2. Informaticien qui recherche à exploiter les faiblesses de la sécurité informatique.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

L'analyse de maître Pascal Agosti[1, 2]

« En juin 2016, un individu (ou un groupe) a exploité une faille dans le code d'un *smart contract* d'une organisation autonome décentralisée (The DAO) développée par Slock.it qui s'appuie sur la blockchain Ethereum et utilise sa monnaie virtuelle, les ethers. Sa mission est de faire du *crowdfunding* en vue de financer des projets d'Internet, des objets (IOT) et des voitures intelligentes. Finalement, le préjudice s'est élevé à près d'un tiers des 168 millions de dollars collectés, soit environ 50 millions de dollars. L'attaquant a respecté le code (informatique) de The DAO et s'est donc trouvé "juridiquement" inattaquable. Comme il n'existe pas d'organe central pour décider des actions à mener, les mineurs de The DAO avaient jusqu'au 14 juillet 2016 pour choisir la solution définitive par un vote. À défaut, l'individu aurait pu récupérer son butin au préjudice des investisseurs. Pour résoudre le problème, Ethereum a recouru à un *hard fork*[3] en juillet 2016 consistant à modifier le code de la blockchain afin de récupérer les ethers "siphonnés" et de les redistribuer à leurs "légitimes" détenteurs. Pour choisir la solution, il n'y a eu qu'environ 20 % des détenteurs d'ethers qui ont pris part au vote. Ce qui semble relativement peu sur le plan de la représentativité.

La faille du système réside essentiellement dans sa gouvernance (inexistante ou incertaine). La question ne se poserait pas dans une blockchain non publique (de consortium ou privée), dans la mesure où la sécurité, le contrôle et l'organisation des pouvoirs de décisions relèveraient de l'organe central (une personne morale) investi de la gouvernance, mais aussi qui engagerait sa responsabilité. L'ensemble de cette organisation serait régi par des statuts et un règlement intérieur de fonctionnement. »

1. Maître Pascal Agosti, avocat, Caprioli Avocats – http://www.caprioli-avocats.com/
2. L'Usine digitale, juillet 2016, http://www.usine-digitale.fr/article/la-blockchain-pose-de-serieux-problemes-de-confiance-de-droit-et-de-securite.N401527
3. *Hard fork*, voir « *fork* » : objet ayant une racine commune avec un second. Ces deux objets, jumeaux au départ, suivent chacun, après séparation, leur évolution propre.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

La blockchain modifiable, utopie ou réalité ?

Cette affaire de *hacking* de The DAO a révélé le besoin de capacités de modifications dans les systèmes de blockchain privée (ou *permissioned*). En revanche, avec la technologie blockchain « conventionnelle », si quelqu'un tente d'opérer un changement sur un bloc, il « casse les maths », ou la chaîne d'algorithmes, que détiennent l'ensemble des blocs. Sauf si un nombre suffisant de participants acceptent le changement, le système effectue un rejet, laissant la blockchain intacte et créant une preuve traçable d'une manipulation. Si un nombre suffisant de participants convient de la modification, alors un *fork* (comme pour Ethereum en juillet 2016) peut être ajouté, avec une branche se terminant là où se situe le bloc défectueux et une autre branche qui continue en avant du bloc corrigé. Après qu'un bloc a été corrigé, tous les blocs suivants doivent être reconstruits, ce qui peut être très perturbateur et très coûteux et, dans certains cas, pratiquement impossible.

Voici pourquoi Accenture a créé en septembre 2016 un prototype d'une nouvelle capacité qui permet à la technologie blockchain de travailler dans des circonstances extraordinaires afin de résoudre les erreurs humaines, de tenir compte des exigences légales et réglementaires, tout en préservant les fonctionnalités de cryptographie. Ce prototype, selon Accenture, représente une avancée significative pour les utilisations de l'entreprise de technologie blockchain, notamment dans le secteur de la banque, de l'assurance et des marchés de capitaux. Il s'agirait donc d'une blockchain modifiable[1] – ce qui va à l'encontre des principes mêmes de la blockchain.

1. Lire à ce sujet l'article « Editing the Uneditable Blockchain : Why distributed ledger technology must adapt to an imperfect world », https://acnprod.accenture.com/us-en/insight-editing-uneditable-blockchain

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Lectures utiles

Voici quelques conseils de lecture sur les sujets abordés jusqu'alors et à venir :

- « La folle histoire d'Ethereum Classic », http://www.blockchaindailynews.com/La-folle-histoire-d-Ethereum-Classic_a24537.html
- « Contrats autonomes et applications décentralisées », http://www.valkenberg.net/contrats-autonomes-et-applications-decentralisees/
- « Ethereum *vs* Bitcoin : les différences », http://blogchain-cafe.com/ethereum-vs-bitcoin-les-differences
- « DLT : alternative aux blockchains Bitcoin et Ethereum », http://www.louisbachelier.org/publications/opinions-debats/blockchain-autres-registres-distribues-avenir-marches-financiers/

Protocoles de consensus distribués

Définition

Comme déjà explicité plus haut, le terme *distributed ledger* (registre ou grand livre distribué) apparaît progressivement en 2014 dans de nombreuses sociétés blockchain ou dans des publications spécialisées pour différencier les blockchains publiques ou historiques (Bitcoin, Ethereum) des nouvelles blockchains plus récentes (privées ou hybrides) et par conséquent plus modernes dans leur conception et plus agiles dans leur usage.

Mais le terme même de blockchain est-il approprié pour une blockchain publique ?

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Avançons un peu plus loin dans le raisonnement et, si vous le voulez bien, abordons ici un point qui me semble crucial pour la compréhension de l'univers blockchain et des technologies qui le composent.

Lorsque nous parlons de blockchain et de chaîne de blocs, désignons-nous la même chose ?

Nous savons qu'une blockchain est une structure de données en « chaîne de blocs », mais ce chaînage n'est en réalité qu'une partie du protocole de registre distribué. Par extension, il serait par conséquent plus « logique » de nommer ces plateformes technologiques, ces blockchains, des « protocoles de registre distribués » (avec registre ouvert ou fermé).

L'aspect essentiel du registre distribué ouvert est par nature la distribution des données et l'efficacité de l'algorithme de consensus qui établit une vérité sur l'état des transactions enregistrées par les différents nœuds du réseau. C'est d'ailleurs de cet algorithme que dérivent la plupart des propriétés du registre distribué.

Ainsi, par exemple, dans l'univers Bitcoin, la sécurité et la décentralisation de la blockchain Bitcoin (registre distribué) proviennent notamment des propriétés de son algorithme de consensus distribué (preuve de travail anonyme ou *proof of work*)… et non de l'aspect chaînage de blocs.

Voici pourquoi, par extension, nous pensons qu'il serait souhaitable de nommer les blockchains des « protocoles de consensus distribués ».

Voici les composantes d'un protocole de consensus distribué :

- un *token* (jeton ; par exemple, une monnaie cryptographique telle que le bitcoin) ;
- un mécanisme de consensus (par exemple, *proof of work* ou preuve de travail) ;

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

- une structure (par exemple, la blockchain) ;
- un réseau de participants (nœuds) ;
- un ensemble de règles (par exemple, protocole Ripple).

Maintenant que nous avons planté le décor et après avoir visité avec Bitcoin et Ethereum ce qu'il est convenu d'appeler les blockchains publiques, voyons les différents types de blockchain.

Les types de blockchain

La question de la blockchain publique ou privée n'est pas récente. Mais le débat est devenu à nouveau d'actualité depuis que les banques, les institutions financières, voire les banques centrales se sont intéressées à la technologie de la blockchain pour expérimenter des applications purement privées.

Blockchain publique *vs* blockchain privée[1]

Blockchain publique (ou historique)

C'est un registre (*ledger*) ouvert à tous. Cette blockchain se caractérise par son ouverture totale : tout le monde peut y accéder et effectuer des transactions et tout le monde peut participer au processus de consensus.

Il n'y a donc pas de registre central, ni de tiers de confiance. C'est le modèle le plus connu, celui qui est à l'origine de la technologie, selon une approche communautaire, voire alternative, de l'économie. Les puristes considèrent que seul le singulier s'applique à cette technologie : on parle alors de *la* blockchain. Son fonctionnement est fondé sur les

1. Lire à ce sujet Vitalik Buterin, « On Public and Private Blockchains », https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

« *cryptoeconomics*[1] », c'est-à-dire la combinaison d'incitations économiques et les mécanismes de vérification en utilisant la cryptographie comme une preuve de travail (PoW) ou preuve de la participation (PoS). La blockchain publique est par nature totalement décentralisée.

Blockchain de consortium ou hybride

Ici, le processus de consensus est contrôlé par un ensemble présélectionné de nœuds (participants).

On pourrait imaginer, par exemple, un consortium de 15 institutions financières, dont chacune gère un nœud et dont au moins 10 doivent signer chaque bloc pour que ce bloc soit considéré comme valide. L'accès à cette blockchain peut être public ou restreint aux participants selon un processus de cooptation. Ces blockchains peuvent être considérées comme « partiellement décentralisées ».

On peut prendre comme exemple de blockchain hybride le consortium R3 CEV dont 50 banques environ sont membres.

Blockchain privée

Enfin, il y a les blockchains totalement privées, dont l'accès d'écriture est délivré par une organisation centralisée (par exemple une banque centrale), mais où les autorisations de lecture peuvent être publiques ou restreintes (privées).

Caractéristiques et consensus

Chaque blockchain est définie par sa communauté, le type de transactions qu'elle autorise, la méthode qu'elle choisit pour valider l'honnêteté du consensus, ainsi que son caractère privé ou public.

1. Néologisme de Vitalik Buterin (Ethereum).

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

- Blockchain publique (ou *unpermissioned blockchain* ou *blockchain mining*) :
  - caractéristiques : réseau public sans intermédiaire, pas de censure ;
  - consensus (*proof of work*) : coûteux, « lent », récompenses intrinsèques au réseau (mineurs).

Blockchains publiques et pertes de transactions

Tous les protocoles de consensus distribués (blockchains hors Bitcoin, Ethereum et variantes) sont des solutions alternatives au problème général de la sécurisation des données dans un registre publique décentralisé. Ils sont tous non seulement plus rapides et plus efficaces que la solution Bitcoin, mais aussi développés avec des méthodes formelles qui donnent la certitude mathématique quant à leur justesse.

Maintenant que nous avons présenté les blockchains publiques et les consensus, nous pensons qu'il est opportun de rappeler que le Bitcoin n'offre pas de preuve mathématique formelle quant à son fonctionnement. Au contraire, il est prouvé que son protocole présente des lacunes d'un point de vue théorique. En effet, dans certains cas, il échoue à résoudre le problème d'accord byzantin.

Il est démontré que dans la pratique (et c'est de notoriété publique, au moins parmi les experts) le Bitcoin peut perdre des données en cas de *fork* (scission) de sa blockchain. Lorsqu'un *fork* se recompose, alors seule la branche la plus longue gagne et est validée, ce qui entraîne la possibilité que les transactions de la branche perdante soient complètement perdues.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

- Blockchain privée (ou *permissioned blockchain* ou blockchain consensus) :
  - caractéristiques : privées ou semi-privées (différents droits d'accès à la plateforme), acteurs connus ou identifiables, industries régulées ;
  - consensus : entre acteurs connus, fonctionnement extrinsèque à la plateforme (pris en charge par le ou les mandataires de la blockchain privée).
- Blockchain Bitcoin :
  - avec monnaie bitcoin : Bitcoin (BTC) ;
  - avec autre monnaie : Factom (Factoids), Mastercoin (MSC), Counterparty (XCP), Namecoin (NMC).
- Blockchain non-blockchain Bitcoin :
  - avec monnaie bitcoin : Blockstream, Truthcoin ;
  - avec autre monnaie : Ethereum (Ether), BitShares (BTS), Truthcoin (Cashcoin), Litecoin (LTC), PayCoin (XPY).
- Blockchain non-blockchain :
  - avec consensus sans minage : Ripple (XRP), Stellar (STR), NXT[1] (NXT), Hyperledger, Tendermint, Pebble, Open Transactions, beAchain.
- Blockchain neutre :
  - services intelligents : Monax (ex-Eris Industries), PeerNova, Codius, SmartContract, SAE, Tezoz, Tillit.

Voici un petit tour d'horizon qui nous a permis de classer quelques solutions existantes mais la liste n'est pas exhaustive, le classement demeurant très subjectif et mouvant.

1. NXT Whitepaper : https://nxtwiki.org/wiki/Whitepaper:Nxt#Proof_of_Stake

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Consensus

Définition

D'une manière globale, un consensus est un accord général positif et unanime au sein d'un groupe de personnes permettant de décider ou d'agir ensemble sans vote préalable ou délibération particulière.

Et nous l'avons déjà écrit, « le consensus informatique dans le domaine des systèmes distribués est un moyen pour les nœuds (participants) de se mettre d'accord sur la validité d'une transaction et de mettre à jour le grand livre avec un ensemble cohérent de faits confirmés[1] ».

D'une façon basique et historique (naissance vers 1970 avec les algorithmes), le consensus demeure fondamental en matière d'informatique distribuée ou de calcul distribué[2], c'est-à-dire là où nous avons un certain nombre de nœuds (participants) qui doivent s'accorder sur une décision. Le principe étant de parvenir à une certaine fiabilité d'un système dans des problèmes de décision distribuée, en présence de pannes.

Ainsi, en informatique théorique, le problème du consensus demande un protocole qui réponde aux critères suivants[3] :

- terminaison : tout processus doit décider une valeur ;
- intégrité : tout processus décide une valeur qui a été proposée par un des processus ;
- accord : tous les processus décident la même valeur.

1. Source : KPMG, George Samman.
2. Le calcul distribué consiste à répartir un calcul ou un traitement sur plusieurs microprocesseurs et plus généralement sur toute unité centrale informatique.
3. Les mécanismes de consensus sont utilisés pour s'assurer que l'ensemble des nœuds du réseau disposent des mêmes informations et que seules les transactions valides soient enregistrées dans les registres distribués.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Un protocole qui peut garantir ces propriétés en présence de moins de *t* pannes est dit « t-robuste ».

Le propos ici n'est pas d'expliquer le fonctionnement d'un « consensus » (algorithmes/mathématiques) mais simplement de montrer que différents consensus existent au sein des blockchains (dites publiques) et des protocoles de consensus distribués (dits blockchains privées).

Lors de notre exposé du fonctionnement de la blockchain Bitcoin, nous avons évoqué le consensus de *proof of work*[1] ou preuve de travail (minage). Or, nous savons désormais qu'il existe des algorithmes de consensus distribués plus efficaces (suivant les cas d'usage) et moins énergivore que le *proof of work*.

La preuve d'enjeu ou de participation

Nous savons que le minage est énergivore et certains acteurs, comme Ethereum, pensent quitter la preuve par le travail pour aller vers la preuve d'enjeu du fait de cette trop grande consommation énergétique due à la grande puissance de calcul nécessaire.

Ainsi, pour valider des blocs, il ne faut plus utiliser de la puissance de calcul et par conséquent « brûler » de l'énergie mais posséder une certaine quantité de crypto-monnaie.

Tour d'horizon des consensus

Pour sauvegarder une vue cohérente du registre (collectivement), il existe un certain nombre d'algorithmes de consensus (classement par date de naissance) :

1. Adam Back, « HashCash – A Denial of Service Counter-Measure », http://www.hashcash.org/hashcash.pdf

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

- **1998 | Preuve de travail** – *proof of work* (PoW)[1] : les utilisateurs doivent exécuter plusieurs fois les algorithmes de hachage ou calculer des puzzles mathématiques selon des algorithmes pour valider les transactions électroniques :
  - Bitcoin (spécificité : tous les nœuds sont anonymes et potentiellement malicieux, donc on a besoin d'une *proof of work* « inutile » en apparence, mais utile à la sécurité du réseau) ;
  - Ethereum (spécificité : *idem* Bitcoin) ;
  - Peercoin et Decred[2] utilisent une méthode hybride PoW/PoS pour tenter de tirer avantage des deux systèmes et de créer un consensus plus robuste.
- **1998 | Paxos**
- **2013 | Preuve d'enjeu** ou de participation – *proof of stake* (PoS)[3] : l'utilisateur doit prouver la possession d'une certaine quantité de crypto-monnaie pour prétendre pouvoir valider des blocs supplémentaires dans la chaîne de blocs et pouvoir toucher la récompense, s'il y en a une, attribuée à l'addition de ces blocs :
  - Projet Ethereum 2017 (Sharding[4]) ;
  - Peercoin[5], preuve d'avoir utilisé la PoS ;
  - (i) Preuve de possession – *proof of hold* (PoH) : plus longtemps vous possédez la monnaie, plus vous avez de droits de validation ;
  - (ii) Preuve d'utilisation – *proof of use* (PoU) : plus vous échangez de la monnaie, plus vous avez de droits de validation ;

1. Système qui lie la capacité du minage à la puissance de calcul.
2. https://decred.org
3. Méthode par laquelle une chaîne de blocs d'une crypto-monnaie vise à atteindre un consensus distribué.
4. Projet Sharding : http://ethereum.stackexchange.com/questions/573/what-is-a-shard
5. https://peercoin.net/index.php?locale=fr

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

- (iii) Preuve d'enjeu/temps – *proof of stake/time* (PoST) : fonction mathématique qui tient compte du temps de possession de la pièce pour définir une probabilité d'être choisi pour valider le prochain bloc de la chaîne de blocs (exemples : Peercoin,Vericoin) ;
- (iv) Preuve enjeu minimum/temps – *proof of minimum aged stake* (PoMAS) : méthode mixte avec pondération(s) ;
- (v) Preuve d'importance – *proof of importance* (PoI) : les utilisateurs qui ont le plus d'enjeu dans la crypto-monnaie sont récompensés (exemple : NEM).

Proof of work versus proof of stake[1]

La *proof of work* (preuve de travail) et la *proof of stake* (preuve d'enjeu ou de possession) sont les deux façons de valider les blocs les plus connues. Elles impliquent deux mécanismes de consensus très différents.

Le processus qui consiste à résoudre un défi informatique imposé par une *proof of work* est appelé *mining* ou minage : on parle de mineurs.

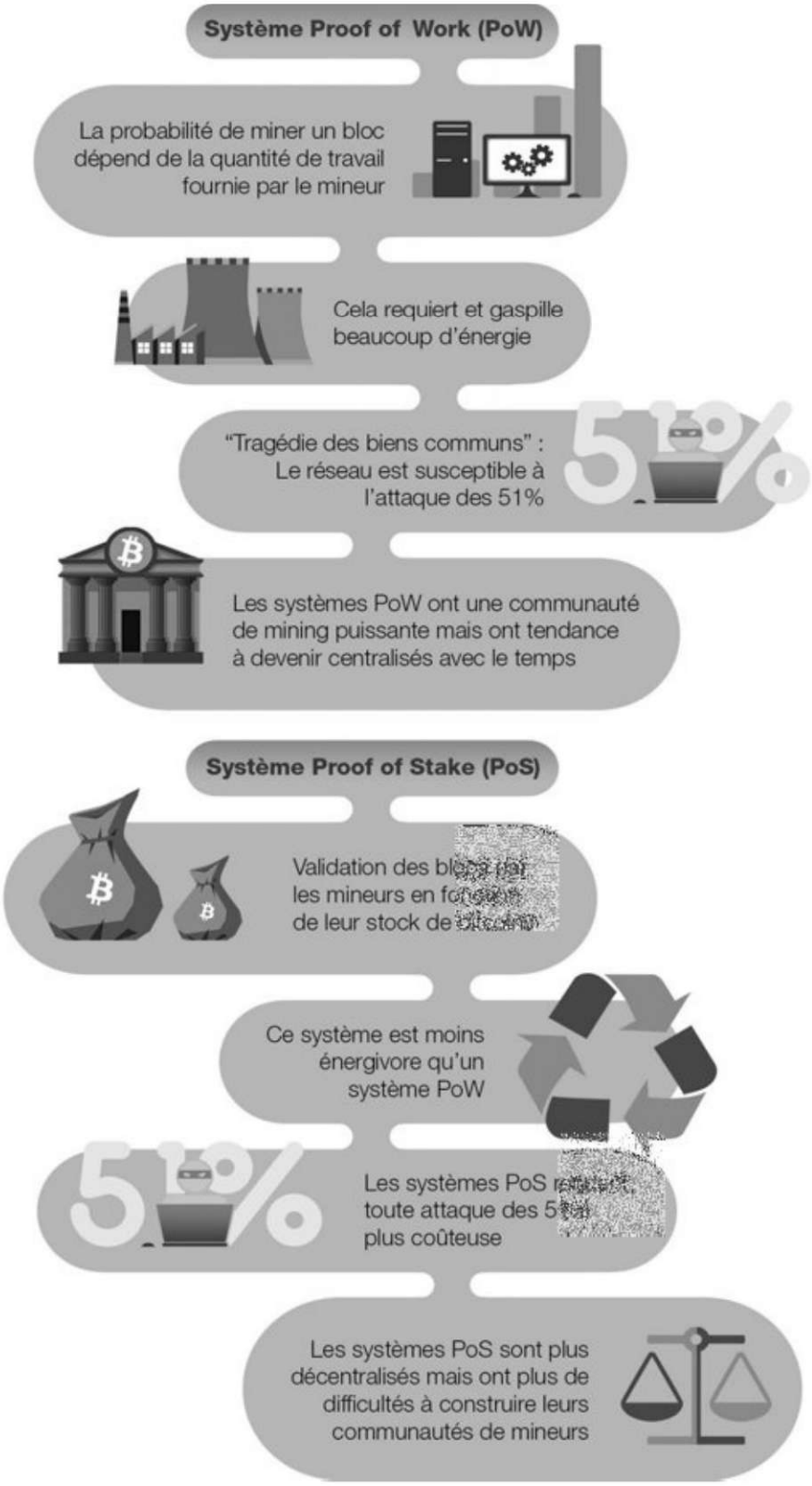
Le processus qui consiste à résoudre un défi informatique imposé par une *proof of stake* est appelé *minting* : on parle de forgeurs.

- **2013 | Délégation de preuve de possession** – *delegated proof of stake* (DPoS) : ici le consensus utilise un système de réputation, on élit par un vote un groupe limité de personnes de confiance. Seules ces personnes ont le droit d'inscrire des blocs et ce, chacune leur tour, dans un ordre

1. PoW *vs* PoS : http://blogchaincafe.com/les-consensus-proof-of-work-vs-proof-of-stake#more-559

Copyright © 2017 Eyrolles.

© Groupe Eyrolles



Copyright © 2017 Eyrolles.

© Groupe Eyrolles

aléatoire[1]. Tous les possesseurs de jetons peuvent voter, les votes sont pondérés par le nombre de jetons que possède le votant.
  - Bitshares[2] ;
  - Graphene[3] ;
  - Steem[4].
- **2013 | Raft**[5] (Paxos dérivé)
  - **preuve d'autorité** : un ou plusieurs nœuds sont autorisés à ajouter des blocs ;
  - **preuve d'activité** (suivant les profils des nœuds) ;
  - **preuve de capacité** (suivant les profils des nœuds) ;
  - **preuve d'ipséité** (exemple beAchain) ;
  - **tolérance aux fautes byzantines** (exemple Hyperledger et beAchain) ;
- **2016 | Juno**[6] (Raft dérivé) – Création JP Morgan
- **2016 | Tangaroa**[7] (Raft dérivé)

1. OCTO : http://blog.octo.com/quel-consensus-dans-une-blockchain-privee/
2. https://bitshares.org/
3. https://bitshares.org/blog/2015/06/15/the-history-of-graphene/
4. https://steem.io/
5. https://raft.github.io/
6. http://www.the-blockchain.com/docs/JP-Morgan-Juno-Distributed-Cryptoledger.pdf
7. http://www.scs.stanford.edu/14au-cs244b/labs/projects/copeland_zhong.pdf

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Consensus entre machines, entre objets par beAchain

Lorsqu'une transaction (demande d'authentification/login, échange de valeurs, partie de contrat spécifique, etc.) est demandée par une ou des machines ou des objets participant à la chaîne, un certain nombre de machines connectées au même moment doivent se mettre d'accord pour décider ensemble si la transaction est acceptée ou pas. Le nombre de machines concernées (voir théorie des graphs acycliques[1]) est paramétrable : plus il est élevé plus le temps de travail pour atteindre le consensus sera long mais plus le résultat sera garanti.

Écosystème

Voici à présent un bref tour d'horizon des dernières innovations (liste non exhaustive) dans ce domaine des blockchains que certains qualifient de blockchains 2.0 – même si, à notre avis, nous sommes beaucoup plus proches de protocoles de registres (ou consensus) distribués que de blockchains (chaînes de blocs).

Lisk – Dapps[2]

Lisk est une jeune entreprise fondée par Max Kordek. Début 2016, elle a levé 14 000 bitcoins en *crowdfunding*. Le projet Lisk, qui présente de nombreuses similarités avec Ethereum[3], a pour but de faciliter le développement et l'hébergement des Dapps (voir encadré ci-après).

1. Voir glossaire : http://www.blockchaindailynews.com/glossary/
   La théorie des graphs acycliques détermine, dans un ensemble d'objets distants les uns des autres et espacés de façon variable, le chemin optimal pour aller de tel objet à tel autre.
2. https://lisk.io/
3. Voir l'article de David Teruzzi, « Lisk : un concurrent d'Ethereum ? », http://www.finyear.com/Lisk-un-concurrent-d-Ethereum_a35894.htm

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Lisk est une plateforme de nouvelle génération qui permet le développement et la distribution d'applications décentralisées écrites en Javascript. Avec Lisk, les développeurs peuvent construire, publier, distribuer et monétiser leurs applications avec une crypto-monnaie interne. Le système ainsi construit utilise une *custom blockchain*, des *smart contracts*, le stockage dans le *cloud* et des nœuds de calcul, le tout à l'intérieur d'une seule solution industrielle.

Lisk est la première solution décentralisée d'application écrite entièrement en Node.js. Elle travaille donc de manière asynchrone et permet de traiter sans retard (apparent) les tâches, comme les transactions réseau. La base de données utilise SQLite pour permettre l'utilisation et l'exécution de *query* complexes. Lisk se base sur HTML5 et CSS3 pour le *frontend*.

L'utilisation de langages standards et bien connus fait que l'écosystème Lisk est disponible en l'état pour des milliers de développeurs sans compétences supplémentaires. N'importe quel développeur web qui connaît déjà Javascript et Node.js peut immédiatement le prendre en main pour construire des applications décentralisées dès le premier jour.

Le but principal de Lisk est de créer un système *plug-and-play* qui permettrait aux développeurs de tout faire : du design, de la conception, du développement, de la publication, de la monétisation, le tout à l'intérieur d'une seule plateforme. En utilisant l'écosystème Lisk, les développeurs peuvent déployer rapidement leurs Dapps Javascript vers le Lisk Hosting & Storage Nodes, être visibles dans le Lisk App Store et avoir un accès immédiat aux Lisk Compute Nœuds pour l'exécution du code. Le tout étant soutenu par l'intégrité et la sécurité qui viennent de la fonctionnalité de consensus des Lisk sidechains.

Toutes les tâches de l'écosystème sont exécutées par les utilisateurs et les délégués de Lisk qui sont payés par un système de

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

facturation automatique interne (ou par le réseau lui-même dans le cas des délégués). La rémunération des nœuds se fait en LSK, la crypto-monnaie propre à Lisk, ou en bitcoins.

Qu'est-ce qu'une Dapp ?

Une Dapp[1] est une application décentralisée fonctionnant au sein d'une blockchain grâce aux ressources mises à disposition par les mineurs. Concrètement, elle permet à des acteurs dont les moyens financiers sont insuffisants pour subvenir aux coûts de déploiement d'une application (énergie, stockage, CPU, maintenance) de la déployer sur une blockchain. De plus, la Dapp a l'avantage d'être flexible sur les ressources utilisées, elle s'adapte à la CPU demandée ou à l'espace de stockage requis.

Stellar Consensus Protocol (SCP)[2]

Stellar.org propose le protocole de consensus stellaire (SCP), une construction pour l'accord byzantin fédéré (Federated Byzantine Agreement – FBA).

SCP s'inspire de Bitcoin et a ajouté la capacité de tolérer des acteurs non rationnels dans un environnement à faible puissance de calcul.

SCP est la première construction sûre pour le FBA et, contrairement à la plupart des approches existantes pour les consensus, elle présente quatre propriétés clés :

- le contrôle décentralisé : en tant que protocole FBA, SCP garantit la sécurité face à un comportement non rationnel

1. Pour en savoir plus sur les Dapps : http://blogchaincafe.com/les-dapps-applications-distribuees-decentralisees#more-443
2. SCP Stellar : https://www.stellar.org/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

et ne nécessite que des ressources informatiques modestes, réduisant ainsi la barrière à l'entrée ;

- la confiance flexible : cela signifie que les utilisateurs ont la liberté de faire confiance à toute combinaison de parties qu'ils jugent bonne ;
- la faible latence ;
- la sécurité asymptotique : ici, la sécurité repose sur les signatures numériques et les familles de hachage dont les paramètres peuvent être réglés de manière réaliste pour protéger le système contre les adversaires avec une grande puissance de calcul. Pour prendre une image, imaginez un mot de passe qui peut croître en longueur de caractère à mesure que la puissance de calcul d'un attaquant augmente.

Ripple[1]

Lancé en 2012, le réseau Ripple permet des « transactions financières mondiales sécurisées, instantanées et presque gratuites, de toute taille sans rejets de débit ». Il prend en charge n'importe quelle monnaie fiduciaire, crypto-monnaie, commodité ou toute autre unité de valeur telles que miles aériens, minutes mobiles, distances de GPS…

Ripple est un protocole[2] pour l'échange de monnaies qu'on pourrait définir de « http pour l'argent ». Comme http, son utilisation est libre et sans licence ; comme le bitcoin, il permet des transactions en argent.

En 2016, Ripple est la troisième plus importante crypto-monnaie par capitalisation boursière, après Bitcoin et Ethereum.

Le protocole Ripple est de plus en plus adopté par les banques et les réseaux de paiement comme la technologie

1. https://ripple.com/
2. The Ripple Protocol Consensus Algorithm : https://ripple.com/files/ripple_consensus_whitepaper.pdf

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

d'infrastructure des paiements. Sur les cinquante plus grandes banques au monde, dix travaillent déjà avec Ripple. Ripple est une blockchain privée (*permissioned*).

IOTA[1]

Alors que l'IoT (*Internet-of-Things*, l'Internet des objets) continue d'élargir le besoin d'interopérabilité et de partage des ressources, IOTA permet aux entreprises d'explorer de nouveaux modèles B2B en faisant de chaque ressource technologique un service potentiel à échanger sur un marché ouvert en temps réel et sans frais.

IOTA est basé sur un nouveau livre distribué, Tangle[2], qui surmonte les inefficacités des conceptions des blockchains actuelles et introduit une nouvelle façon de parvenir à un consensus dans un système pair à pair décentralisé. Pour la première fois, grâce à IOTA les gens peuvent transférer de l'argent sans frais. Cela signifie que même des nanopaiements infinitésimalement petits peuvent être réalisés à travers IOTA.

IOTA est conçu pour fonctionner avec d'autres blockchains comme Bitcoin ou Ethereum et est actuellement en version bêta[3].

Quelques caractéristiques :

- La structure des données ne prend pas la forme d'une blockchain, c'est-à-dire d'une chaîne de blocs contenant des

1. https://www.iotatoken.com/
2. Voir glossaire : http://www.blockchaindailynews.com/glossary/
3. Si vous souhaitez en savoir plus sur IOTA et IOTAtoken, nous vous conseillons la lecture des deux articles suivants : « IOTA, pour en finir avec la blockchain », http://www.blockchaindailynews.com/IOTA-pour-en-finir-avec-la-blockchain-_a24438.html et « IOTAtoken : une tangle crypto-currency », http://blogchaincafe.com/iotatoken-une-tangle-crypto-currency#more-1057

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

transactions. À la place, on y trouve un DAG[1] (*Directed Acyclic Graph*) nommé Tangle. IOTA est une *tangle-based cryptocurrency*.

- Les transactions émises par les nœuds du P2P vont former le Tangle, c'est-à-dire que les transactions forment le grand livre sous forme de DAG[2].
- Lorsqu'une nouvelle transaction arrive, le système doit approuver deux transactions précédentes. Ces approbations, représentées par des arêtes, contribuent à sécuriser le réseau.
- S'il n'y a pas de bord dirigé entre une transaction A et une transaction B, mais qu'il y a un chemin de longueur ≥ 2 de A à B, alors on dit que A approuve indirectement B.

Hyperledger[3]

« *Make blockchain real for business.* »

Hyperledger est un projet *open source*, né en décembre 2015, grâce à l'impulsion de plusieurs grands acteurs (Accenture, Airbus, Fujitsu, Digital Asset, IBM, Intel, JP Morgan, R3CEV…) et géré par la Linux Foundation. L'ambition du projet est de fédérer les efforts pour créer une technologie blockchain, ou plus précisément une technologie des registres distribués, répondant aux besoins spécifiques des entreprises. Il réunit 100 membres (fin 2016) et a enregistré la croissance la plus rapide de tous les projets de la Linux Foundation[4]. Ces membres sont à la fois des entreprises ou des consortium technologiques (IBM, Intel, Fujitsu, Digital Asset, R3, Red Hat…) et des entreprises diverses (Airbus, JP Morgan, BNP, ABN Amro).

1. Voir glossaire : http://www.blockchaindailynews.com/glossary/
2. Dans ce cercle fermé des DAG, IOTA présente quelques similitudes avec la solution française beAchain qui est en cours de développement et prévoit de lancer sa version 1 en février 2017.
3. https://www.hyperledger.org
4. https://www.hyperledger.org/announcements/2016/11/30/hyperledger-hits-100-member-milestone

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Le principal projet hébergé par Hyperledger est appelé Fabric dont une part importante du code provient des laboratoires d'IBM qui a décidé de le mettre à disposition en *open source*. Il vise à la création de *permissioned ledger* pour des contextes industriels. Dans un *permissioned ledger*, à la différence d'une blockchain publique (comme le sont par exemple les monnaies cryptographiques Bitcoin et Ethereum), seuls des acteurs autorisés peuvent participer au consensus en devenant un nœud du système. En effet, dans des contextes industriels réglementés, l'identification et l'autorisation des participants s'imposent.

Hyperledger a pour ambition de devenir une source de confiance pour les solutions blockchain à destination des entreprises grâce à une vaste communauté développant des composants et des plateformes modulaires. Le projet n'a pas pour but de mettre en place un registre partagé directement utilisable mais plutôt de mettre à disposition des entreprises les piliers fondateurs pour construire des blockchains « *business-ready* » (prêtes à être utilisées par l'entreprise). Chaque acteur, ou plutôt chaque consortium d'acteurs, pourra alors bâtir sa propre blockchain adaptée à ses besoins. Lors de la création, ils décident communément de toutes les caractéristiques du registre distribué : le type d'enregistrements ou de contrats auto-exécutables, les critères de validation, le mécanisme de consensus, les standards de confidentialité, les méthodes d'accès…

En plus des caractéristiques classiques de la blockchain (registre distribué, décentralisé, immuable, possibilité d'inscrire des *smart contracts*), la technologie d'Hyperledger contient par défaut des fonctionnalités supplémentaires très utiles pour les applications d'entreprise :

- protection de l'anonymat (impossibilité d'associer une identité à une transaction ou des transactions entre elles) : il est possible de ne pas dévoiler l'identité de l'auteur d'un enregistrement publié sur le registre commun, cela est

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

indispensable dans certains cadres réglementaires spécifiques ou pour garantir la compétitivité ou le savoir-faire ;

- algorithme de consensus personnalisable : le mode de consensus peut être modifié en fonction du cas d'usage. Cela permet d'atteindre des niveaux de performance proches des systèmes non distribués (en termes de volumétrie, de débit et de temps de réponse) ;
- confidentialité : le contenu des transactions peut être chiffré pour préserver la confidentialité des échanges. Grace à cette propriété, il est possible de décider à quelles informations a accès chaque acteur du réseau ;
- auditabilité : le système prévoit l'auditabilité des transactions ;
- scalabilité : Hyperledger est conçu pour assurer de grands volumes de transactions et une viabilité dans le temps.

Exemples d'applications

Le code d'Hyperledger a déjà été utilisé dans différents projets. HSBC et Bank of America ont, par exemple, testé la mise en œuvre d'une solution pour rationaliser les lettres de crédit en finance. Le projet réplique un échange de lettre papier entre l'entreprise exportatrice, l'entreprise importatrice et leurs banques respectives *via* l'utilisation de contrats auto-exécutables.

En France, le Crédit Mutuel Arkéa prévoit de l'utiliser pour assurer le partage des informations KYC (*Know Your Customer*, connaître son client) sur ses clients en interne. La banque néerlandaise ABN AMRO, quant à elle, prévoit d'utiliser Hyperledger pour uniformiser les informations dans la chaîne de restructuration et de redressement financier. Walmart a pour ambition de l'utiliser pour améliorer la traçabilité de la viande porcine en Chine, Japan Exchange Group pour les règlements post-marché, l'entreprise finlandaise Kouvola voudrait coupler Hyperledger avec des objets connectés pour rendre plus intelligente la chaîne logistique. UBS, après avoir

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

expérimenté la technologie blockchain pendant environ deux ans, prévoit d'utiliser la technologie des registres distribués Hyperledger pour créer un système import-export mondial de transaction.

Interledger[1]

Ce protocole, développé par Ripple Labs, pour relier les blockchains aux registres distribués, permet des paiements à travers des réseaux différents et utilise des dépôts fiduciaires pour traiter les mouvements de fonds entre deux livres séparés. Le protocole d'Interledger est formellement modelé utilisant TLA+[2] et est aussi utilisé par Amazon pour traiter le cas de systèmes critiques.

Contrairement à l'approche Bitcoin ce protocole n'exige aucun système de coordination globale de blockchain.

Tendermint[3]

Tendermint est un protocole[4] qui permet de répliquer de manière sécurisée et cohérente une application sur de nombreuses machines. Tendermint fonctionne même si jusqu'à un tiers des machines échouent de manière arbitraire (consensus BFT).

Tendermint se compose de deux éléments techniques principaux : un moteur consensuel blockchain et une

1. https://interledger.org/
2. TLA+, acronyme de Temporal Logic of Actions (« logique temporelle des actions »), est un système de méthode formelle pour les algorithmes parallèles et distribués.
3. https://tendermint.com/
4. « Tendermint: Consensus without Mining », http://the-blockchain.com/docs/TendermintConsensuswithoutMining.pdf

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

interface générique d'application. Le moteur consensus, appelé Tendermint Core, garantit que les mêmes transactions sont enregistrées sur chaque machine dans le même ordre. L'interface d'application, appelée Tendermint Socket Protocol (TMSP), permet de traiter les transactions dans n'importe quel langage de programmation. Contrairement à d'autres solutions blockchain et consensuelles, les développeurs peuvent utiliser Tendermint pour la réplication de machine d'état BFT quels que soient le langage de programmation et environnement de développement.

Monax[1] (ex-Eris industries)

Monax est un cadre qui a pour but de permettre la création et l'utilisation d'applications web distribuées sans serveur. Chaque application utilise une blockchain distribuée créée sur le réseau Ethereum qui se comporte comme un serveur pour réaliser un consensus partagé. L'interface utilisateur est construite utilisant HTML, CSS et Javascript. N'importe quelle sorte d'application web existante peut être recréée sur la plateforme Eris, par exemple un forum, une plateforme web de *crowdfunding*, une place de marché, etc.

Corda[2] by R3CEV

Début décembre, R3CEV a publié le code source de Corda, son *distributed ledger* pour les banques et compagnies financières. La version test contient cinq types de contrats intelligents et les développeurs soulignent que le nouveau système n'est pas basé sur une blockchain classique.

Selon le livre blanc, « Corda est une plateforme de comptabilité distribuée pour l'enregistrement et le traitement des

1. https://monax.io/
2. https://www.corda.net/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

accords financiers. [...] Contrairement à Bitcoin et Ethereum, Corda n'ordonne pas de transactions utilisant une chaîne de blocs et, par implication, n'utilise pas de mineurs ou de preuve de travail (consensus). Au lieu de cela, chaque état pointe vers un "oracle" ou "notaire", qui est un service garantissant qu'il ne signera une transaction que si tous les points d'entrée sont conformes.

Les utilisateurs du réseau n'auront pas accès au registre de toutes les opérations, ne voyant qu'un sous-ensemble des données gérées par le système. Les données sont confirmées si au moins deux acteurs du système sont en consensus à ce sujet, tandis que toute combinaison d'acteurs est autorisée à participer au processus de consensus pour un enregistrement donné.

Pour accéder aux données, les clients Corda pourront utiliser des clés composites. La plateforme leur permet de fournir des clés supplémentaires et des combinaisons à des tiers participant à l'opération.

La caractéristique principale de Corda en tant que système est une capacité intrinsèque à exécuter des contrats intelligents. Sa version actuelle offre aux utilisateurs cinq types de contrats intelligents appelés Cash, Commodity, Commercial Paper, Interest Rate Swap and Obligation. Tous les contrats peuvent être liés au temps, disent les développeurs : « Les contrats à durée déterminée avec les notaires (oracles) devraient être synchronisés avec les horloges atomiques de l'Observatoire naval américain. »

Les utilisateurs peuvent combiner et modifier des modèles pour créer des contrats uniques adaptés à leurs besoins. L'équipe Corda a publié un didacticiel sur la façon de coder un contrat simple avec les éléments disponibles dans la version actuelle.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Actuellement, la plateforme en est au stade de l'essai. Afin de poursuivre la recherche et le développement, R3CEV a obtenu le soutien des principales banques mondiales, dont Bank of America, JP Morgan, Credit Suisse, Barclays, Deutsche Bank, HSBC, Citi, Commerzbank et Société Générale (Santander et Goldman Sachs ont quitté le consortium fin novembre[1]).

beAchain[2], une blockchain orientée objets (BOO)

beAchain est une solution blockchain (en cours de développement) qui propose à ses utilisateurs de développer eux-mêmes leurs propres applications *peer-to-peer* sécurisées sans aucune compétence informatique.

Une blockchain « orientée objets » signifie qu'elle est conçue pour permettre à des objets connectés – ordinateurs, tablettes, smartphones, mais aussi tous les appareils relevant de l'IoT (Internet des objets) : capteurs, véhicules, habitat, vêtements, appareils électroménagers, drones, etc. – de dialoguer entre eux, de comparer leurs données, de s'interroger les uns les autres et, au final, de décider selon des algorithmes particuliers si une transaction est acceptée ou pas, ce qui permet de réaliser à terme plusieurs dizaines de milliers de transactions par seconde. Pour ce faire, beAchain s'appuie sur des protocoles spécifiques privilégiant l'ultra-compacité de ses modes de cryptages et l'ultra-rapidité de ses processus.

En facilitant les regroupements d'objets dans des groupes d'objets associés (GOA[3]), beAchain permet de créer des organisations temporaires virtuelles (Quick Virtual Organization,

1. R3CEV : http://www.blockchaindailynews.com/Goldman-Sachs-confirme-son-depart-de-R3_a24794.html
2. http://www.beachain.com
3. Groupes d'objets associés, voir glossaire : http://www.blockchaindailynews.com/glossary/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

QVO[1]) qui sont des modèles de développement économique alternatifs à l'entreprise industrielle. Sans adresse, sans murs, sans stocks, sans charges ni frais et sans masse salariale, la QVO est une organisation décentralisée autonome de production où les machines connectées peuvent monter leurs propres business, pilotées par des outils de contractualisation créés par les utilisateurs. Adossées à des outils d'intelligence artificielle développés en interne, ces interfaces de contractualisation leur permettent d'écrire leurs *smart contracts* en langage naturel (français, anglais…) que les algorithmes beAchain traduisent en codes à exécuter par les machines. Tout contrat peut ainsi être testé et réécrit par toutes les parties concernées avant son lancement public.

Tout objet sur beAchain est à la fois capable de détenir de la crypto-monnaie, d'engager des contrats commerciaux avec d'autres objets (*smart contracts*), d'être appelé pour réaliser une tâche particulière ou de participer à un consensus transactionnel. Il est par exemple possible d'invoquer dans un applicatif toutes les voitures et rien que les voitures. Ou de ne s'adresser qu'aux capteurs thermiques. Ou encore d'exclure tous les smartphones d'un protocole particulier. Les authentifications de machines contractantes sont sécurisées par des preuves d'identité incassables (*quantum-resistant*) selon des jeux de clés privées/clés publiques garantissant une protection optimale.

À la fois privés, publics ou hybrides selon les protocoles appelés, les domaines d'application de beAchain vont des usages industriels (automobile, énergie, gestion de stocks, traçabilité produits) aux services en ligne (assurances, transferts de valeurs, authentifications), de l'organisation d'événements (culturels, éducatifs, sportifs) aux médias (*pay-per-view*), du transport

1. Quick Virtual Organization, voir glossaire : http://www.blockchaindailynews.com/glossary/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

(VTC, colisage, billetterie) aux contractualisations d'objets à objets (partage/authentification fichiers STL, pilotage imprimantes 3D) et des plateformes de partage/fablabs aux outils de citoyenneté numérique (votes, participations citoyennes, délibérations, outils de codécision).

Les QVO, organisations virtuelles temporaires

Construites sur le même modèle et la même technologie qu'une QVE, QVO est un modèle beAchain de développement beaucoup moins orienté business ; adaptées à la conception/création d'événements de types culturels, politiques, sociaux, sportifs, elles se donnent un objectif et des étapes pour atteindre ce dernier.

Elles se rapprochent conceptuellement parlant de la DAO Ethereum à la différence qu'elles ne s'inscrivent pas dans la durée mais dans l'objectif. Un exemple est une « QVO Paris-New York[1] » où l'objectif est de créer un vol transatlantique de façon entièrement ouverte et décentralisée.

Pour résumer

Nous voici arrivés au terme de ce chapitre 2 consacré aux registres, protocoles et consensus qui sont l'évolution technologique de la blockchain Bitcoin qui permet des échanges transactionnels monétaires de pair à pair en crypto-monnaie, le bitcoin.

Inventé en 2008 par Satoshi Nakamoto, Bitcoin se présente comme une plateforme décentralisée permettant, par un certain nombre de protocoles et de technologies, de garantir

1. http://beachain.com/BEACHAIN-QVO-Paris-NewYork.pdf

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

confiance et sécurité dans les échanges en supprimant tout tiers de confiance (banques en l'occurrence).

Les transactions sont cryptées, anonymes, sécurisées, inviolables et leur historique est encrypté dans les chaînes de blocs réparties entre toutes les machines sans qu'aucun serveur n'ait à les collecter, les stocker, les centraliser et les redistribuer. C'est une technologie parfaitement horizontale où les transactions ne sont plus validées par une instance extérieure, mais par un consensus direct entre pairs.

Très vite, un constat s'impose : le potentiel de la blockchain[1] est immense et ses applications presque infinies, à la condition de pouvoir élargir son champ d'action, limité dans Bitcoin aux échanges financiers.

En 2014, un jeune développeur,Vitalik Buterin, crée Ethereum, une plateforme blockchain inspirée de Bitcoin mais conçue de telle façon qu'on puisse imaginer toutes sortes d'autres utilisations. Commence alors à émerger le concept « d'ordinateur mondial » : toutes les machines connectées à Ethereum peuvent échanger, partager, collaborer, mutualiser pour produire des données qui seront distribuées horizontalement sous forme cryptée, encapsulées dans des blocs.

Simultanément et progressivement d'autres blockchains voient le jour : Lisk Ripple, IOTA, Hyperledger, Interledger, Tendermint, Monax, Corda, beAchain… De nouveaux horizons s'ouvrent aux expérimentations.

1. Pour les bitconistes historiques, il n'existe qu'une seule blockchain. Pour certains éthereumiens, il n'y en a que deux. Pour tous les autres, il en existe autant qu'il y a de registres distribués (DLT) à transactions horizontales P2P consensuelles, qu'elles soient publiques, hybrides ou privées.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Quelles que soient leurs spécificités (publiques ou privées, avec ou sans mining), leurs protocoles (PoW, PoS) ou leurs algorithmes, toutes ont en commun de présenter des caractéristiques similaires : les données sont décentralisées, encryptées en blocs, réparties uniformément sur le réseau, et les transactions, que ce soit des échanges financiers, des exécutions de codes, des computages de datas, sont approuvées par consensus entre acteurs de la blockchain.

Par son protocole de plateforme, la blockchain promet que ce qui capturera, ce qui créera demain de la valeur, ce n'est pas (ou alors très marginalement) qu'un véhicule autonome électrique puisse dialoguer avec notre smartphone pour le paiement d'une course, mais qu'une plateforme universelle permette à tout utilisateur de créer lui-même à la demande les applicatifs dont il a besoin, et autant qu'il en aura besoin, que ce soit pour des usages individuels ou collectifs (entreprises, collectivités, associations) *via* des protocoles contractualisés (*smart contracts*) sécurisés, intangibles et infalsifiables.

On pénètre alors dans des domaines où l'Internet des objets (IoT), l'intelligence artificielle (IA) et les technologies *peer-to-peer* (blockchain) convergent pour produire des échanges économiques décentralisés, non propriétaires, ouverts, basés sur des systèmes de confiance réciproque et de paiements horizontaux en temps réel garantis par le protocole lui-même.

Entrons maintenant dans la pratique…

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Chapitre 3

La blockchain en pratique

« L'innovation systématique requiert
la volonté de considérer le changement
comme une opportunité. »

Peter Drucker

Copyright © 2017 Eyrolles.

Copyright © 2017 Eyrolles.

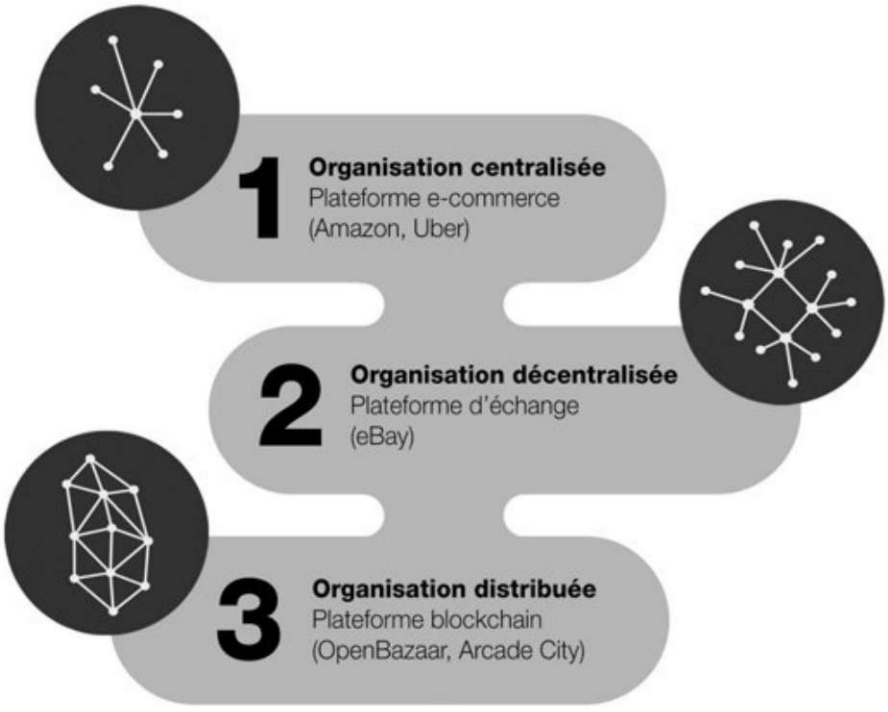
Cas d'usage, applications

À ce stade de l'évolution de la technologie blockchain, les disruptions potentielles et les possibilités de transformer les business sont tellement importantes qu'il est encore très difficile de prendre le recul nécessaire pour les percevoir.

Toutefois, dans le domaine de la finance, nous pourrions préciser que les principaux bénéficiaires de ces disruptions devraient être les acteurs se situant aux extrémités de la chaîne de valeur (émetteurs, investisseurs) et que les intermédiaires (tiers de confiance) devront se repositionner sur des fonctions à valeur ajoutée.

Principes de la technologie blockchain

La blockchain, solution inédite, décentralisée, sécurisée et transparente, permet de stocker, d'échanger, d'authentifier et



Copyright © 2017 Eyrolles.
© Groupe Eyrolles

de vérifier des informations pour un coût faible et supporté par l'utilisateur (donc sans tiers de confiance). Mais quels en sont les champs d'application possibles ?

Centralisation *versus* décentralisation

La décentralisation est un concept important qui n'est pas propre à la blockchain Bitcoin. La notion de « centralisation *versus* décentralisation » se pose dans une grande variété de technologies numériques. Par exemple Internet, qui est un système décentralisé, puis les courriels dont le noyau est un système décentralisé basé sur le protocole SMTP (Simple Mail Transfer Protocol), un standard ouvert (dans le cas de la messagerie instantanée et de la messagerie texte, nous avons un modèle hybride qui ne peut être catégoriquement décrit comme centralisé ou décentralisé) ; quant aux réseaux sociaux, malgré les nombreux efforts concertés des amateurs, des développeurs et des entrepreneurs pour créer des alternatives au modèle centralisé, ils demeurent des systèmes centralisés – comme Facebook et LinkedIn qui dominent ce marché. En réalité, ce conflit date de bien avant l'ère du numérique et nous observons une lutte similaire entre ces deux modèles dans l'histoire de la téléphonie, de la radio, de la télévision et du cinéma.

Dans la pratique, aucun système n'est purement décentralisé ou purement centralisé.

Par exemple, le courrier électronique est fondamentalement un système décentralisé basé sur un protocole standardisé, SMTP, et quiconque le souhaite peut exploiter un serveur de messagerie de sa propre initiative. Pourtant, ce qui s'est passé sur le marché, c'est qu'un petit nombre de fournisseurs de messageries électroniques centralisés sont devenus dominants. De même, alors que le protocole Bitcoin est décentralisé, les services tels que les échanges Bitcoin, qui permettent de convertir

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

des bitcoins avec d'autres monnaies, le logiciel de portefeuille (*wallet*), ou un logiciel permettant aux personnes de gérer leurs bitcoins peuvent être centralisés ou décentralisés à des degrés divers.

Du grand livre distribué au réseau distribué et à l'organisation distribuée

Comme nous l'avons vu précédemment, la blockchain est un réseau distribué ou un registre distribué (*distributed ledger*) ou encore une plateforme pour une organisation distribuée. Au fil des évolutions technologiques, nous sommes passés d'organisations centralisées (Amazon, Uber, plateformes e-commerce) à des organisations décentralisées (eBay) puis, grâce à l'avènement de la technologie blockchain, à des organisations distribuées[1] (OpenBazaar[2], Arcade City[3]) dans lesquelles tous les participants (nœuds) interagissent sans aucune autorité centrale, ni contrôle centralisé et où chaque nœud possède une copie de la base partagée (blockchain).

Le consensus distribué

Le principal problème technique à résoudre dans la construction d'un système distribué, quel que soit le cas d'usage, est l'obtention d'un consensus distribué. Cette notion même de consensus caractérise les blockchains et crée des différences notables entre certaines technologies blockchain. Ainsi les

1. Ces organisations distribuées sont au cœur du projet DAO d'Ethereum. Pour la première fois, nous voyons apparaître une forme de société entièrement décentralisée mais qui, à ce jour, n'existe que sur la blockchain Ethereum et ses participants n'interagissent entre eux que sur la blockchain. Ce type de société est 100 % transparente, les comptes et les échanges entre participants étant publics.
2. https://openbazaar.org/
3. https://arcade.city/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

blockchains Bitcoin ou Ethereum font appel au consensus *proof of work* (ou preuve de travail ou minage[1]), tandis que d'autres blockchains telles que Casper font appel au consensus *proof of stake* (preuve de détention).

Le champ d'application de la technologie blockchain est extrêmement vaste mais ne signifie pas pour autant qu'on puisse y recourir pour tout et n'importe quoi et surtout sans se poser la question du modèle à adopter et de la forme de gouvernance à mettre en œuvre. Ainsi, tous les usages ne nécessitent pas de recourir à la « preuve de travail », qui implique une communauté importante et impose un coût énergétique plus que substantiel (voir la notion de minage dans le chapitre 2).

La désintermédiation

Le principe de désintermédiation ou suppression du tiers de confiance est au cœur de la technologie blockchain. En effet, cette technologie fonctionne sans intermédiaire.

Pour donner un exemple, dans le cas d'une transaction entre deux individus sans blockchain, une banque vérifie que le payeur a bien les fonds qu'il affirme détenir et accepte ou non la transaction. La banque joue le rôle d'intermédiaire et de tiers de confiance.

En revanche, si les deux individus effectuent cette transaction *via* un système reposant sur une blockchain, c'est le système lui-même qui vérifie l'échange. Cette technologie sert donc à certifier des informations, des échanges, des transactions quelle que soit leur nature sans avoir besoin de faire appel à un tiers de confiance. Aucune manipulation n'est possible, car il faudrait pour cela modifier l'ensemble des points de stockage de la blockchain.

1. Voir glossaire : http://www.blockchaindailynews.com/glossary/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Adopter le principe des livres comptables partagés tout en se « débarrassant » de l'intermédiation financière entraîne le fait qu'une transaction, acceptée ou rejetée, devient le fruit d'un consensus distribué et non d'une institution centralisée.

Certains observateurs prédisent que la blockchain, s'affranchissant des tiers de confiance, devrait « horizontaliser » nos activités.

L'analyse de Gilles Babinet[1]

« La blockchain s'inscrit dans une véritable révolution anthropologique qui va au-delà de la révolution technologique à l'œuvre dans nos sociétés. Dans cette nouvelle ère qui commence à émerger, symbolisée par des concepts comme l'*open source* ou les fablabs, la blockchain peut jouer un rôle essentiel : elle permet en effet de faire à la transaction ce qu'Internet a fait à l'information, grâce à sa capacité à certifier des transactions de manière décentralisée… »

Ce qu'on observe aujourd'hui avec les blockchains, c'est un report de la confiance, traditionnellement acquise aux institutions, vers des communautés d'utilisateurs, dans un vaste mouvement d'horizontalisation de la société.

La sécurité

La sécurité provient du caractère décentralisé et distribué du système : les informations ne sont pas stockées dans un point unique, mais diffusées à l'ensemble du réseau.

Cette technologie est utilisée dans le cadre d'un réseau d'appareils (ordinateurs, smartphones, objets intelligents, etc.) tous liés entre eux de près ou de loin.

1. Gilles Babinet est serial-entrepreneur et Digital Champion de la France à la Commission européenne. Voir https://blockchainfrance.net/2016/01/22/la-blockchain-pour-horizontaliser-le-monde/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Ainsi dans le cadre de la blockchain Bitcoin, chaque participant (nœud) à ce réseau est identifié par une adresse, attribuée lorsqu'il rejoint le système, et qui sera utilisée lors d'une transaction.

En ce qui concerne les éventuelles failles sécuritaires de la blockchain, je vous renvoie à la lecture de l'encadré sur l'attaque à 51 % dans le chapitre 2[1].

La transparence et l'immutabilité

La blockchain libre et gratuite est transparente[2] : elle permet à tout le monde d'accéder au code source de la plateforme, à l'information et à l'historique de tous les échanges ou événements actés depuis la création de la blockchain.

Dans un système « blockchainé » les écritures sont irrévocables et infalsifiables[3]. En d'autres termes, une fois que quelque chose a été enregistré dans ce système, il sera stocké en permanence et sera disponible à la consultation pour tous les participants (nœuds).

Les essais cliniques

Les essais cliniques, bien que vitaux, ont vu leur intégrité et leur transparence de plus en plus remises en question au cours de ces dernières années. Le système de transparence

1. Vous pouvez aussi lire à ce sujet l'article « Une épée de Damoclès sur le Bitcoin », http://www.scilogs.fr/complexites/epee-de-damocles-bitcoin/
2. Pour en savoir plus, lisez « Transparency Overlays and Applications » (http://dl.acm.org/citation.cfm?id=2978404), une étude très intéressante à propos de la transparence dans des environnements distribués et en particulier la blockchain Bitcoin.
3. Lire, à propos de l'immutabilité, l'article portant sur la tentative d'Accenture d'« effacer » des données dans certains cas exceptionnels : « Accenture tue l'innovation », http://www.blockchaindailynews.com/Blockchain-Accenture-tue-l-innovation_a24489.html

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

idéal serait celui qui empêcherait les entreprises pharmaceutiques et les chercheurs de falsifier les données des essais.

Pour répondre à cette attente, les chercheurs de l'université de Cambridge[1] ont créé un système basé sur une blockchain afin de vérifier indépendamment les uns des autres les protocoles des essais cliniques.

La clé de ce travail est l'immutabilité de la blockchain. La preuve de concept[2] de l'université de Cambridge est donc conçue pour s'assurer que ceux qui mènent des recherches ne s'écartent pas de l'essai réel en apportant des modifications au protocole après la réalisation des tests dans le but de faire correspondre les résultats effectifs aux résultats souhaités.

L'utilisation d'un tel système permettrait de satisfaire aux exigences de la déclaration d'Helsinki[3] qui demande que tous les essais cliniques soient enregistrés et publiés sur une base de données accessible au public, tout en évitant les pratiques de manipulation de données pouvant nuire à l'intégrité de la recherche publiée. Comme le processus est rentable et peut être automatisé, il est fort probable que les sociétés pharmaceutiques et les chercheurs universitaires tireront profit des essais cliniques enregistrés sur un système blockchainé.

La traçabilité

Rappelons simplement que la blockchain est un registre actif, chronologique, distribué, vérifiable et protégé contre la falsification par un système de confiance répartie. Par conséquent ce qui y est inscrit est ineffaçable et traçable.

1. http://cambridge-blockchain.com/
2. PoC ou *proof of concept* (preuve de concept) est une démonstration de faisabilité, une réalisation courte ou incomplète d'une certaine méthode ou idée pour démontrer sa faisabilité. C'est une étape importante pour aboutir à un prototype pleinement fonctionnel.
3. http://www.wma.net/fr/20activities/10ethics/10helsinki/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Ainsi nous pourrions appliquer ce principe de traçabilité dans de multiples domaines tels que, par exemple, les aliments, les médicaments, les œuvres d'art, les métaux précieux, et apporter une vraie traçabilité sans avoir recours à de multiples échanges papier ou dématérialisés, sources d'erreurs et de fraudes.

Dans le domaine des œuvres d'art, Deloitte Luxembourg a mis au point, en mai dernier, une alternative technologique aux traces écrites qui attestent la provenance d'une œuvre d'art et de ses déplacements. Cette alternative est l'application ArtTracktive. Elle propose un registre distribué permettant de tracer la provenance et la localisation des œuvres d'art de valeur. Cette preuve de concept basée sur la blockchain assure la gestion des interactions entre les différentes parties concernées de l'artiste ou le propriétaire de l'œuvre, en passant par les transitaires, les douanes, les galeries d'art et les musées jusqu'aux acheteurs potentiels.

Ainsi appliquée au marché de l'art, la technologie blockchain permet un enregistrement fiable et une parfaite traçabilité de l'historique complet du parcours d'une œuvre d'art, de sa création, en passant par ses expositions et ses achats successifs.

L'authentification, la notarisation

Un objet acheté ou vendu, un brevet enregistré, une marque déposée, etc., tous ces transferts d'objets, d'actifs, de documents, de propriété, de contrats sont authentifiés car enregistrés dans la blockchain. On peut de plus y ajouter le propriétaire ou le déposant et joindre l'heure, le jour et l'année grâce à la notarisation native de la blockchain.

Sur ces questions, la start-up française Blockness[1] travaille à l'élaboration de solutions pour tracer la provenance et la

1. http://www.blockness.io

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

propriété d'objets avant tout transfert (donation, cession) mais aussi pour assurer l'authentification de processus (qualité, ISO, etc.).

Blockchain Delaware Initiative

Le Delaware a pour ambition de développer l'utilisation de la technologie blockchain pour l'ensemble des actes notariés des entreprises, en particulier les pactes d'actionnaires relatifs aux levées de fonds des start-up en croissance. Les actes tels que l'enregistrement des sociétés, des actions, la gestion des tables de capitalisation et la communication entre les actionnaires seront gérés grâce à la nouvelle technologie. Des procédures peu risquées sont privilégiées pour le démarrage pour ensuite aborder des problèmes plus compliqués.

Cette initiative a été lancée en mai 2016 avec la start-up Symbiont[1].

Diverses applications

Dressons une liste non exhaustive des diverses applications de la technologie blockchain[2].

Liste d'applications (classement par usage)[3]

(Nous avons spécifié entre parenthèses les noms de certains acteurs qui développent ces applications.)

1. https://symbiont.io/
2. Vous pouvez retrouver les liens web des acteurs travaillant à ces applications et plus encore dans l'annexe en fin d'ouvrage.
3. Voir également le « Top 250 des compagnies & startups blockchain » mis à jour régulièrement : http://www.blockchaindailynews.com/Top-250-blockchain-companies-startups_a24712.html

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

- Actifs – gestion digitale (Colu)
- Applications, preuve de propriété de modules utilisés pour le développement d'applications (Assembly, MyPowers)
- Art – authentification des œuvres d'art (Verisart)
- Assurance – microcontrats (Czam)
- Avis – authentification des avis sur Internet (The World Table, Asimov)
- Cadastre – gestion (Factom)
- Cartes prépayées (BuyAnyCoin)
- Chaîne d'approvisionnement (Skuchain, ThingChain, Caravaggio, Cognizant, Consentio, Fluent, Kouvola Innovation, Modum, Open Trade Docs, Synechron, Zerado)
- Collaboration autour de projets logiciels (BlockchainValley)
- Contenus – diffusion (Alexandria)
- Contrats – digitalisation de contrats (Colu)
- Contrats – gestion contrats et commandes (UbiMS)
- Contrefaçon – lutte contre la contrefaçon (TheRealMcCoy, Chainlink, BlockVerify)
- Contrefaçon (Blockness, Blockverify)
- *Crowdfunding* pour projets blockchain (Koinify, BlockchainValley)
- Diamants – gestion (Everledger)
- Diplômes – authentification des diplômes (KeeeX, dipl.me)
- Documents – authentification de documents, preuves d'existence, preuve de propriété de contenus numériques (Ascribe, Artplus, blockai.com, blockness.io, bitproof.io, ChainyLing, crypto Public Notary, factom.org, KeeeX, proofofexistence.com, remembr.io, Stampery)

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

- Données – bases de données publiques (Mayor Chains)
- Données – analyse des données (Belem.io)
- Données – blockchain des données (KeeeX)
- e-commerce – plateformes disruptives (OpenBazaar)
- Énergie – compteur électrique intelligent (E-Energy Center)
- Énergie – énergie renouvelable et économie de partage (TransActive Grid, powerledger.com, SolarCoin)
- Fidélité – carte de fidélité (Ribbit.me)
- Fidélité – compte de points (Gyftblock)
- Fiduciaire – gestion dépôts fiduciaires (PlayCoin, NewSystemTechnologies, Fundes)
- Finance – transactions financières (SETL, FactoryBanking)
- Identités – authentification des identités (ShoCard)
- Identités – gestion (Ascribe,Verisart, Onename)
- Identités digitales (Onename, Trustatom, FollowMyVote)
- Immobilier – gestion des actifs immobiliers (Blockness.io, Bitproof, Blocknotary)
- Information – audit, traçabilité informations (Factom)
- Internet alternatif (ZeroNet)
- Internet des objets – IoT (IOTA, beAchain,Adept, Filament, Hyperledger)
- Jeux (Spells of Genesis,Voxelnauts)
- MarketPlace – plateforme de création marketplace (NXT)
- Media streaming (Streamium)
- Médical – gestion de dossiers médicaux (BitHealth)
- Médical – information médicale (BitHealth)
- Messagerie (Getgems, Sendchat)

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

- Mining (21 inc., Bitfury)
- Musique (Ujo, Peertracks, BitTunes Music on the Blockchain)
- Noms de domaines – gestion (Namecoin)
- Objets – gestion (Blockness.io, Slock.it)
- Paiement – paiement en ligne simple et sécurisé (Alipay)
- Parts – monétisation des parts dans les start-up (Founderbeam)
- Prédictions – gestion, prédiction de marché (Augur)
- Prêts entre particuliers (MoneyCircles)
- Propriété – sécurité digitale pour le transfert de propriété (Symbiont, Mirror, Secure Asset, Bitshares, Coin-e, equityBits, DXMarkets, MUNA)
- Propriété intellectuelle (Blockness.io, Monegraph, Bitproof)
- Réseau d'affaires (Debune)
- Réseaux sociaux P2P (DATT, Synereo)
- Signature électronique (BlockSign)
- *Smart grid*, *smart cities*, villes intelligentes, bâtiments intelligents (L03 Energy, Enerchain, ElectriCChain)
- Stockage d'or (Bitgold)
- Stockage décentralisé, cloud virtuel (Storj, BigchainDB, Sia.tech)
- Traçabilité (Blockness.io, Blockpharma, Provenance)
- Transport de personnes (aeCar, la'Zooz)
- Uber ubérisé (Arcade City)
- Vie privée – gestion de la vie privée *via* des entités digitales (ShoCard, Uniquid)
- Vote (Voatz, Belem, Neutral Voting Bloc, civicdApp.com, cryptovoter.com, v-initiative.org, followmyvote.com, unchain.voting)

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

La blockchain, tout le monde en parle, peu de monde l'a vue – un peu comme l'Arlésienne de Daudet. Et pourtant, les projets d'utilisation sont nombreux et variés, un peu dans tous les secteurs d'activité. C'est d'ailleurs pour cela que cette technologie dispose de potentiels de développement très importants. Mais encore faut-il passer de l'intention aux actes.

Revue non exhaustive des applications possibles, voire déjà en production

Les projets sont trop nombreux pour les recenser tous. Ce qu'il convient de retenir, c'est leur diversité, dans les domaines les plus courants de la vie. Ce qu'ils ont tous en commun : la sécurisation du transfert et de l'archivage des informations de façon quasi absolue. Ce qui est *a priori* une bonne chose. Mais ce que l'on ne voit pas (encore) venir, c'est le profond changement de mode de vie et de pensée qu'apporte cette technologie. Car en supprimant le risque (de fraude, de perte, d'erreur…), elle supprime le doute, et quelque part ce qui fait que l'homme est un être doué d'une intelligence et d'une conscience, et non une simple machine.

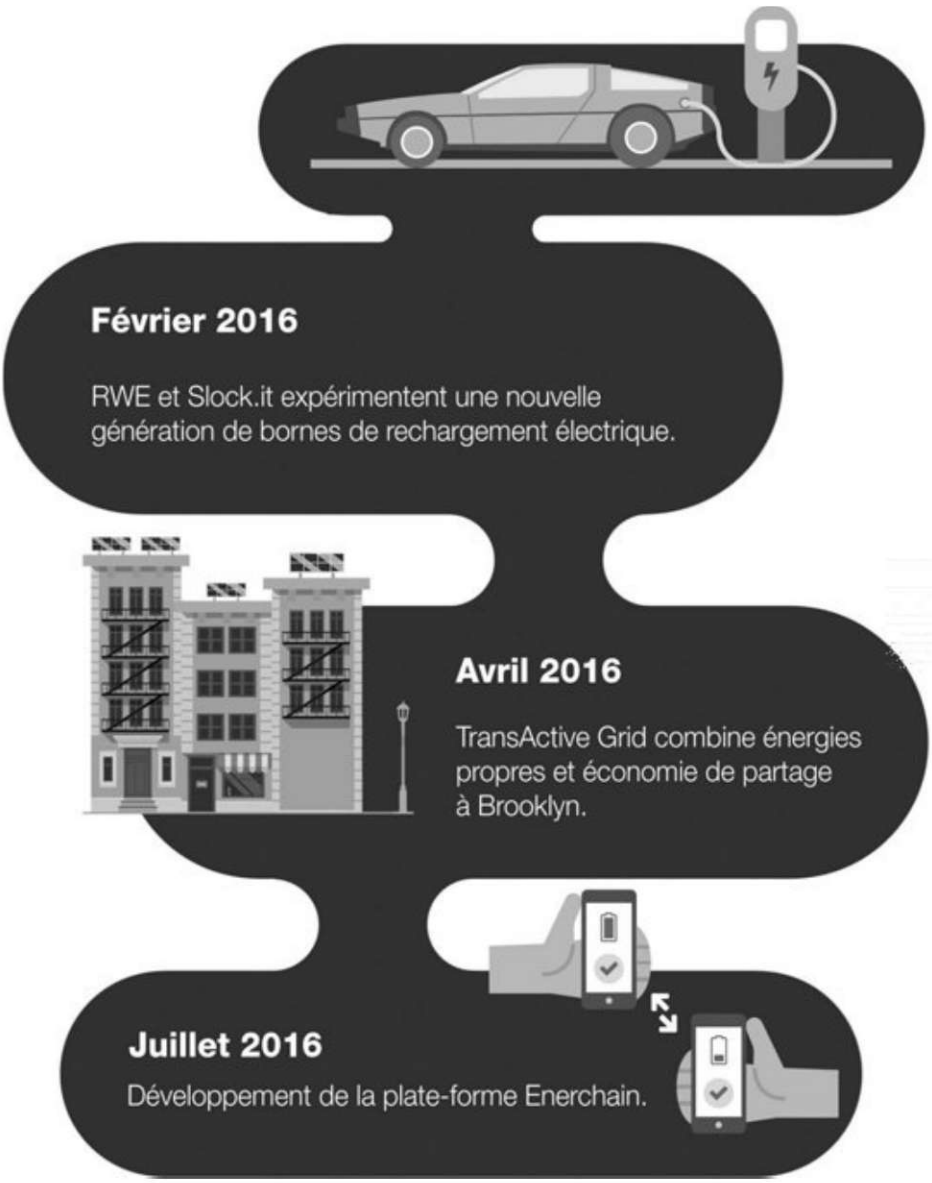
Mais le potentiel futur des applications blockchain évolue encore. Qui aurait imaginé la plupart de ces applications il y a encore quelques mois ? Et quelles applications émergeront d'ici trois, six ou neuf mois ? Les deux ou trois prochaines années devraient être consacrées à l'expérimentation mais nul doute qu'elles nous réserveront leur lot de disruption « blockchainéenne ».

Il semble bien, au regard de tous ces projets naissants, que la technologie blockchain soit là pour s'installer durablement et transformer profondément notre économie et notre société.

Détaillons quelques applications parmi les plus significatives.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Énergie



L'énergie n'est pas, loin s'en faut, l'objet principal du battage médiatique autour de la blockchain, mais elle représente certainement l'industrie où le plus d'applications vont se développer.

Dans l'énergie, la multiplication des auto-producteurs pose d'importants problèmes aux réseaux de distribution traditionnels, conçus historiquement de façon univoque. La solution

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

est celle de la multiplication des réseaux locaux intelligents, les *smart grids*[1].

En février 2016, le conglomérat allemand RWE[2] a annoncé une expérimentation[3] avec la start-up Slock.it autour d'une nouvelle génération de bornes de rechargement électrique. En France, Engie conduit des expérimentations sur le sujet, notamment dans la traçabilité des flux (eau, gaz, électricité).

En avril 2016, une initiative, née à Brooklyn et soutenue par l'État de New York, combine énergies propres et économie de partage. Ce *micro-grid*[4] a été développé par la joint-venture TransActive Grid. Celle-ci est composée de deux entreprises : L03 Energy[5], qui développe des réseaux d'énergie solaire, et ConsenSys[6], spécialisée dans la blockchain Bitcoin. Dans le cas présent il s'agit de donner la possibilité aux citoyens de se réapproprier leur production énergétique, par l'établissement de mini-communautés énergétiques autonomes ; pour cela, des capteurs enregistrent l'historique de la création énergétique à un point précis, et le transmettent aussitôt sur la blockchain Ethereum. Des *smart contracts* peuvent ensuite régir les règles d'utilisation de cette énergie et les tarifs des producteurs.

---

1. Si nous devions anticiper sur la vision prospective que nous avons de la blockchain (voir le chapitre suivant), nous ajouterions que le *smart grid*, s'il est associé à un système distribué de très nombreuses microcentrales, est désigné comme l'un des cinq piliers de la « troisième révolution industrielle » annoncée, notamment par Jeremy Rifkin. Ce qui revient à dire que la révolution blockchain qui se profile passera par le monde de l'énergie.
2. https://www.rwe.com/web/cms/en/8/rwe/
3. Partenariat Slock.it et RWE : https://blog.slock.it/partnering-with-rwe-to-explore-the-future-of-the-energy-sector-1cc89b9993e6#.cxxxl7p5m
4. *Micro-grid* : microréseaux électriques intelligents (produire de l'électricité à l'échelle de son quartier).
5. http://lo3energy.com/
6. https://consensys.net/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Ces initiatives ne sont pas de simples expérimentations sans avenir. En effet, une étude parue en avril 2013 et réalisée par Navigant Research[1] conclut que les projets de *micro-grids* sur l'ensemble du monde pourraient rapporter plus de 40 milliards de dollars par an en 2020, soit quatre fois plus qu'en 2013.

En juillet 2016, Ponton[2], une start-up allemande, a développé la plateforme Enerchain[3], le premier marché européen d'énergie sur blockchain. Enerchain permet d'envoyer des ordres de façon anonyme. Les contreparties cliquent sur leur écran pour conclure une transaction, toutes effectuées en pair à pair, et par conséquent sans aucun tiers de confiance.

En octobre 2016, lors de l'événement Hackenergy[4] 2016, qui s'est déroulé à Groningen aux Pays-Bas, a été présenté un système de négociation d'énergie de type pair à pair (P2P) qui se nomme EcoCoin. Ce système commercial est basé sur la blockchain *open source* Hyperledger (voir le chapitre 2).

Les 3 et 4 novembre 2016, lors de l'événement EMART Energy 2016 qui s'est tenu à Amsterdam, le premier échange européen d'énergie de mégawatts-heures sur une blockchain a été exécuté par le belge Yuso[5] et le néerlandais Priogen[6].

Citons également ElectriCChain[7] qui est un projet porté par Chain of Things[8], un consortium de recherche ouvert. ElectriCChain a pour objectif de mettre en place un outil

1. http://www.navigantresearch.com/newsroom/worldwide-microgrid-market-will-surpass-40-billion-in-annual-revenue-by-2020
2. http://www.ponton.de/
3. http://enerchain.ponton.de/
4. http://www.h4ckenergy.com/
5. http://www.yuso.be/index-fr.html
6. http://priogen.com/
7. http://www.electricchain.org/
8. http://www.chainofthings.com/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

public et sécurisé permettant le suivi de l'énergie solaire en temps réel et à l'échelle mondiale. En pratique, des crédits d'énergie solaire sont transférés à des enregistreurs locaux (connectés aux panneaux solaires), eux-mêmes connectés à un nœud de la blockchain. L'information se retrouve de fait partagée sur le réseau mondial.

Traditionnellement, l'industrie de l'énergie a toujours été lente à adopter des nouvelles technologies. Mais ce secteur est aujourd'hui en pleine mutation numérique et de nombreuses entreprises sont prêtes à exploiter les nouveaux développements technologiques pour relever les nouveaux défis. Les services publics essaient de comprendre comment participer à ce nouveau monde de l'énergie distribuée.

Traçabilité alimentaire

Quelques projets sont en cours, dont le plus important est celui lancé en octobre 2016 par Walmart, IBM et l'université de Tsinghua qui ont signé à Pékin un accord pour explorer la traçabilité et l'authenticité de la chaîne d'approvisionnement alimentaire en utilisant la technologie blockchain[1]. Nous avons ici affaire à trois acteurs de poids dans une économie où la traçabilité alimentaire est cruciale et surtout perfectible.

Lutte contre le piratage des films, de la vidéo et de la musique

Avec l'Internet, le téléchargement des œuvres artistiques est devenu banal, bien que réglementé. L'arrivée des plateformes de téléchargement et de streaming Spotify, Apple Music ou Deezer a déréglé tout le système des droits d'auteur dans l'industrie musicale. S'il est dans un grand nombre de pays illicite de télécharger de la musique ou des films sans passer par des

1. http://www.blockchaindailynews.com/IBM-et-WalMart-explorent-la-blockchain-pour-la-securite-alimentaire_a24646.html

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

sites versant des redevances aux artistes et producteurs, la réalité est toute différente. Par exemple, la dernière saison de la série *Games of Thrones* a été téléchargée illégalement plus de 14 millions de fois.

Le business model de cette industrie est en train de profondément changer du fait de la perte des revenus issus des droits d'auteur. La technologie de la blockchain permet de lutter contre la piraterie.

Tel est le but de la start-up australienne Veredictum[1] pour l'industrie cinématographique ou encore de Revelator[2] pour l'industrie musicale[3]. Il s'agit de proposer aux producteurs d'enregistrer les films, scripts et autres travaux de création dans la blockchain *via* un système de tokenisation[4] (en cours de test). Ainsi, toute utilisation illégale de ces informations sera automatiquement reconnue car non validée par la chaîne de blocs. La même solution est en train d'être testée pour les vidéos sur des plateformes de type YouTube.

Authentification des marchandises, notamment des médicaments

Le marché de la contrefaçon est prospère et Internet facilite le commerce illégal de ce type de biens. Toutes les marchandises ou presque sont copiées dès lors qu'elles représentent une valeur marchande. Un cas particulier est celui des médicaments,

1. https://scripts.veredictum.io/
2. http://revelator.com/
3. Lire également « Music On The Blockchain (Foreword by Nick Mason, Pink Floyd) » : http://www.blockchaindailynews.com/Music-On-The-Blockchain-Foreword-by-Nick-Mason-Pink-Floyd_a24414.html
4. La tokenisation est le procédé qui permet de remplacer une donnée critique par un élément équivalent (jeton ou *token*) qui n'aura aucune valeur intrinsèque ou signification exploitable une fois sorti du système.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

compte tenu des enjeux liés à la santé. Environ 10 à 30 % des médicaments fournis dans les pays en développement sont des « faux médicaments ».

L'Organisation mondiale de la santé estime ainsi à 700 000 le nombre de décès par an provoqués par des médicaments contrefaits. Un moyen de lutter contre ce phénomène serait de créer un système universel garantissant la traçabilité des médicaments. La start-up française Blockpharma[1] propose une solution permettant de vérifier instantanément *via* son smartphone l'authenticité de la boîte de médicaments achetée.

Archivage des données médicales et partage du dossier médical

Les informations médicales de chacun d'entre nous sont des données à la fois très personnelles et intimes méritant un traitement confidentiel, mais dont la connaissance par des tiers se révèle indispensable en cas d'urgence, accident, malaise ou toute autre situation de perte de conscience. Comment s'assurer que les premiers secours disposent de l'ensemble du dossier médical sans que celui-ci ne soit à la portée du premier venu ?

Une start-up californienne, Blockchain Health[2], propose d'archiver les données médicales des individus « cobayes » travaillant avec des centres de recherches médicaux.

La blockchain permet de mieux gérer et sécuriser l'accès au dossier médical partagé (DMP), grâce au système de *smart contracts*. Tel est le projet MedRec[3] aux États-Unis.

On peut même aller plus loin, et prévoir l'accès au dossier médical *via* la blockchain en ayant recours à un système de multi-signature permettant d'ouvrir le dossier grâce à la

1. http://www.blockpharma.com/
2. https://blockchainhealth.co/
3. https://www.pubpub.org/pub/medrec

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

signature conjointe du patient et du médecin. Et de prévoir que cet accès requiert un certain nombre de signatures (clés privées) pour en ouvrir l'accès. C'est en partie ce qui motive le projet Enigma[1] en cours de développement au MIT qui vise plus généralement à la protection des données privées.

Cadastre

On sait que le cadastre permet de cartographier les délimitations de propriétés. Et donc à l'État de prélever des impôts en cas de succession ou de vente… Sans cadastre, non seulement l'État perd des revenus, mais les propriétaires des terrains ne peuvent pas certifier que ceux-ci leur appartiennent.

Or, en Afrique mais aussi en Amérique latine, de nombreux pays ne disposent pas de cadastre, ou tout au moins de cadastre fiable. Pour résoudre ce problème, l'ONG Bitland[2] a annoncé le lancement d'un projet de cadastre numérique au Ghana qui permettrait aux propriétaires d'arpenter leurs terres *via* un GPS et d'enregistrer leurs actes fonciers sur une blockchain. Il ne s'agit encore que d'un projet, comme c'est le cas au Honduras qui avait indiqué vouloir faire appel à cette technologie avec la société Epigraph[3].

Administration

Tous les États, grands comme petits, doivent gérer de multiples documents pour leurs citoyens et administrés : documents relatifs aux impôts bien sûr, mais aussi divers documents officiels comme permis de conduire, carte d'identité, visa et autres.

Or, si l'on voit émerger de plus en plus de projets de numérisation des documents administratifs, y compris en France, rares

1. http://www.enigma.co/
2. http://landing.bitland.world/
3. http://epigraph.io/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

encore sont les projets qui indiquent vouloir archiver ces documents dans la blockchain.

Tel est pourtant le cas à Dubaï où le prince héritier vient d'annoncer en octobre 2016 la mise en place sur blockchain de ces informations, notamment afin de pouvoir vérifier les visas. Cela permettra d'économiser jusqu'à 25,1 millions d'heures de production des agents administratifs par an.

Identité

L'identité numérique permet de faire le lien entre un objet numérique et une identité physique (des personnes, des entreprises et des objets). Le but est de pouvoir réaliser une vérification de l'identité pour les besoins par exemple des banques, des transports, mais aussi de dématérialiser les certificats de naissance et de décès, de créer un système de réputation virtuel.

Plusieurs start-up se sont lancées dans des projets d'identification numérique *via* la blockchain, comme ShoCard[1] en matière d'enregistrement des données issues des documents d'identité pour les besoins des contrôles aux aéroports (ou autres plateformes de transport).

Dans un autre genre, la start-up américaine Onename[2] permet de se créer une « identité virtuelle » sur Internet *via* la blockchain : cela ressemble à un compte Facebook qui permet d'ouvrir des comptes sans avoir à renseigner d'adresse e-mail, d'identifiant ou de mot de passe, l'identité n'étant pas centralisée sur les serveurs d'une société, mais sur la blockchain. Seul son propriétaire peut y accéder au moyen d'une clé privée. Il devient alors impossible à Facebook (et consorts) de « revendre » notre identité à des tiers à des fins commerciales.

1. https://shocard.com/
2. https://onename.com

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

L'analyse de maître Pascal Agosti[1]

« Le règlement européen eIDAS sur l'identité et les services de confiance contient à la fois des règles juridiques et des normes techniques de sécurité. Ce règlement contribue à la confiance dans le cadre des transactions électroniques. Pour ce faire, les services de confiance au rang desquels figurent les certificats, les cachets, horodatages électroniques s'appuient sur le recours à des prestataires de services de confiance (PSCo), des tiers en charge de la fiabilité des outils techniques précités. Cette démarche centralisatrice semble antithétique de la logique de la blockchain, par essence décentralisée quand elle est publique.

De plus, si le règlement eIDAS nécessite une construction en amont de la confiance (par la mise en place d'une architecture et des processus de vérification contraignants pour susciter une confiance conditionnelle), la technologie de la blockchain présuppose la confiance qui peut donc être "déçue" en aval par des anomalies ou des défaillances (confiance aveugle).

Pourtant, cette antinomie n'enlève rien à leur complémentarité. La technologie de la blockchain peut être requise dans le cadre de la confiance dans les transactions comme par exemple pour les journaux dans les systèmes d'archivage électronique. De plus, la confiance partagée par le réseau permettrait de balayer le reproche fréquent rencontré par les PSCo du risque de partialité et d'absence d'indépendance ou d'autonomie.

Dès lors, plutôt que de les opposer, mieux vaut déterminer comment elles peuvent être utilisées ensemble, étant précisé que certains points restent essentiels comme :

- l'importance juridique de pouvoir imputer une action (sur une blockchain) à une personne déterminée. Il s'agit de l'un des fondements pour engager la responsabilité civile d'une personne ;
- l'horodatage des transactions est essentielle pour assurer leur traçabilité (et leur cohérence). Par exemple, en matière comptable, à défaut de cohérence dans la succession des dates des transactions, une comptabilité informatisée pourrait être remise en cause. Il en irait de même pour une blockchain utilisée pour un cadastre par exemple.

1. Avocat, Caprioli Avocats, http://www.caprioli-avocats.com/ Voir aussi sur le sujet É. Caprioli, *Signature électronique et dématérialisation (Droit et pratiques)*, LexisNexis, 2014.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

En outre, il ne faut pas omettre la question essentielle de la protection des données à caractère personnel comme notamment le respect du principe de "droit à l'oubli" que l'on retrouve à l'article 17 du règlement du 27 avril 2016 (effacement des données). Ce principe a été consacré par la Cour de justice de l'UE dans l'affaire Google Spain du 13 mai 2014[1]. Or, dans la blockchain, on dispose d'un registre public qui suppose la conservation des données sans possibilité de les effacer et sans réelle possibilité de déterminer leur localisation géographique. Des questions juridiques passionnantes en suspens... »

Paiement

L'un des enjeux les plus importants pour les années à venir en matière bancaire consiste à maîtriser la fraude lors des paiements électroniques. Or, malgré les sécurités développées par les banques comme la technologie 3D Secure, les fraudes continuent d'être massives. C'est donc un domaine où tous les acteurs veulent se développer. À ce jour, l'initiative la plus aboutie, outre le bitcoin, est Ripple[2]. Ripple permet d'effectuer des transactions financières sécurisées, instantanées et presque gratuites, de toute taille, sans rejet de débit. Il prend en charge n'importe quelle monnaie fiduciaire, crypto-monnaie, marchandise ou toute autre unité de valeur telle que miles aériens, minutes mobiles, distances de GPS…

Règlement livraison

Bien d'autres applications de la blockchain sont possibles, notamment dans les marchés financiers et les systèmes de règlement livraison.

1. CJUE, gde ch., 13 mai 2014, aff. C-131/12, Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos e.a. : JurisData n° 2014-009597.
2. https://ripple.com/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Force est de constater que plus de trente années après la dématérialisation des titres, la France accuse un retard certain en matière de technologie post-marché. Aujourd'hui, pour combler ce retard, la blockchain pourrait être, non seulement le registre de l'émission et des mouvements, mais aussi celui de l'inscription des titres (ou des devises). Ainsi une blockchain remplirait tout à la fois les fonctions d'un registre, d'un marché, et d'un « compte de titres ».

C'est ce que propose la start-up londonienne SETL[1] qui permet de remplacer les dépositaires centraux de titres, les chambres de compensation et les systèmes de règlement/livraison.

Financement participatif [2]

« Nous allons profiter de l'ordonnance sur la réglementation financière, chargée de dépoussiérer les bons de caisse et de créer des minibons, pour expérimenter sur la blockchain », a déclaré le ministre de l'Économie Emmanuel Macron lors des Assises de la finance participative[3] le 29 mars 2016[4]. Cette annonce s'est matérialisée dès le mois suivant par l'introduction en droit français de la blockchain, décrite comme « un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations[5] ».

Réservés pour l'intermédiation aux plateformes agréées « conseiller en investissements participatifs (CIP) » ou

1. https://setl.io/
2. Par Léo Lemordant, CEO Enerfip, www.enerfip.fr et maître Diane Hervey, avocat au barreau de Paris.
3. http://www.crowdlending.fr/assises-financement-participatif/
4. Cité dans le communiqué de presse de l'association professionnelle Financement participatif France.
5. Article L.223-12 du Code monétaire et financier (« CMF ») issu de l'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

« prestataire en services d'investissements (PSI) », les minibons sont dotés d'un régime juridique hérité des bons de caisse à la sécurité renforcée. Avec une échéance maximum de cinq ans, les minibons sont des titres nominatifs réservés aux sociétés anonymes (SA), par actions simplifiées (SAS) ou à responsabilité limitée (SARL) justifiant d'au moins trois exercices comptables et au capital intégralement libéré. Ils peuvent être souscrits par des particuliers comme des institutions et des entreprises. Pour pouvoir procéder aux émissions, les plateformes peuvent accéder au fichier bancaire FIBEN de l'émetteur afin d'évaluer la santé financière de l'entreprise et d'effectuer pleinement leur mission de conseiller en investissements[1].

La véritable innovation des minibons réside dans leur mode de distribution, puisque l'ordonnance permet aux plateformes d'utiliser un dispositif fondé sur la technologie blockchain, pour la première fois reconnue par la législation en France. À bien des égards, le secteur du financement participatif est en effet un terrain d'expérimentation idéal pour la blockchain en droit français.

Tout d'abord, car le volume de transactions à traiter par les CIP est relativement faible, du moins par rapport aux marchés réglementés et organisés, ce qui rend sans objet certains des reproches fréquemment adressés à la blockchain tels que la relative lenteur de la confirmation des transactions, les doutes sur la capacité de la technologie à traiter de très importants volumes de transactions (*scalability*), ou encore le caractère énergivore du procédé[2].

1. Xavier Delpech, « Le régime juridique des bons de caisse modernisé », *Dalloz actualité*, 10 mai 2016.
2. Du moins pour les blockchains fonctionnant en preuve de travail (*proof of work*) et non en preuve de détention (*proof of stake*).

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

D'autre part, car les transactions opérées par les CIP *via* la blockchain ne posent pas de difficulté au regard du droit à l'oubli ou encore de la propriété intellectuelle, corps de règles difficilement conciliables avec l'inaltérabilité et la décentralisation de la blockchain publique[1]. Les minibons en particulier, en tant qu'actifs financiers nouvellement créés et ne ressortissant pas de la catégorie des instruments financiers et de leur règlementation stricte, se prêtent parfaitement à l'expérience.

Les acteurs du financement participatif sont intéressés par la blockchain pour la tenue de registre. Les sociétés émettrices de titres de créances comme les minibons, mais aussi les obligations et les actions, sont tenues de garder à jour un registre des souscripteurs. Si cette tenue de registre peut être déléguée à un tiers sous certaines conditions, la blockchain vient l'améliorer substantiellement. En effet, si nombre d'acteurs prévoient de maintenir un registre sous forme de base de données standard, la blockchain peut se révéler être un *back-up* très intéressant, car se présentant sous une forme radicalement différente des bases de données classiques. Ainsi, il est inenvisageable que les deux systèmes rompent simultanément, alors que la synchronisation des deux systèmes est à la fois simple à réaliser et quasi instantanée – en tout cas à l'échelle de la fréquence des transactions. De plus, la blockchain permet une grande transparence dans la tenue de registre. Le délégataire est responsable du registre, mais l'émetteur n'a pas besoin du délégataire pour y avoir accès et produire les documents légaux.

1. Olivier Hielle, « La technologie Blockchain : une révolution aux nombreux problèmes juridiques », *Dalloz actualité*, 31 mai 2016.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Plusieurs acteurs français du financement participatif se sont déjà penchés sur ce cas d'usage. Cependant, à l'automne 2016, seul Enerfip[1], plateforme d'investissement participatif dédiée au développement durable, avait réalisé un *proof of concept* applicable en l'état dans son business. Enerfip propose d'utiliser la blockchain de Bitcoin, en privatisant son accès, la plateforme jouant alors le rôle de tiers de confiance[2].

BNP Paribas Securities Services a annoncé étudier le cas d'usage du minibon en partenariat avec trois plateformes, mais également la tenue de registre des titres non cotés[3]. Il s'agit ici d'utiliser plutôt une blockchain privée.

De son côté, l'association professionnelle Financement participatif France a noué un partenariat avec la Caisse des dépôts et consignations, afin de tester pour les minibons l'utilisation de *smart contracts* basés sur Ethereum.

Toutefois, les modalités d'application, qu'un décret devrait préciser, n'ont toujours pas été publiées par l'État (à date de fin novembre 2016), et les acteurs restent dans l'expectative[4].

1. https://enerfip.fr/
2. Le livre blanc publié par Enerfip intitulé « La Blockchain, nouveau levier du financement participatif » est disponible gratuitement au téléchargement sur https://blockchain-explorer.enerfip.fr/livre-blanc
3. Communiqué de presse : https://group.bnpparibas/communique-de-presse/bnp-paribas-securities-services-renforce-plateforme-blockchain-titres-entreprises-cotees
4. Voir également par extension « L'Assemblée nationale habilite le gouvernement à légiférer sur la blockchain par ordonnance » : http://www.finyear.com/L-Assemblee-Nationale-habilite-le-gouvernement-a-legiferer-sur-la-blockchain-par-ordonnance_a36403.html

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

L'analyse de maître Pascal Agosti[1]

« L'ordonnance n° 2016-520 du 28 avril 2016 relative aux bons de caisse intègre la première définition légale d'un type particulier de Blockchain "pour l'émission et la cession de minibons". Ces opérations pourront (au choix du prestataire qui pourra opter pour un registre papier) "être inscrites dans un dispositif d'enregistrement électronique partagé permettant l'authentification de ces conditions, notamment de sécurité, définies par décret en Conseil d'État" (art. L. 223-12 du CMF).

Un décret en Conseil d'État est censé venir déterminer les conditions de nature à assurer la tenue d'un registre électronique distribué, fiable, sécurisé et susceptible d'être audité. À titre indicatif, le décret n° 2016-1453 du 28 octobre 2016 relatif aux titres et aux prêts proposés dans le cadre du financement participatif (JO du 30 octobre 2016) n'aborde pas ce point. »

Vote numérique distribué

Le plus grand défi des votes électoraux en ligne demeure sans nul doute la sécurité. Or, grâce à la technologie blockchain, un électeur pourrait vérifier que son vote a bien été transmis avec succès tout en restant anonyme pour le reste du monde.

De nombreux États utilisent des machines à voter qui ont plus de dix ans et qui sont non seulement obsolètes et défaillantes mais également de plus en plus coûteuses à entretenir. Du fait de cette défaillance, la fraude électorale grandit, affaiblissant le tissu même de la démocratie.

Nos gouvernements devraient s'emparer de la technologie blockchain pour apporter plus de transparence dans les

1. Voir aussi É. Caprioli, « Consécration légale de la "blockchain" dans les bons de caisse », Comm. com. électr. juin 2016, comm. 58 ; P. Agosti, « La blockchain a sa première définition légale » (http://www.usine-digitale.fr/article/la-blockchain-a-sa-premiere-definition-legale.N392352) ; H. de Vauplane, « La blockchain et la loi » (http://www.finyear.com/La-Blockchain-et-la-loi_a35403.html))

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

processus électoraux et surtout plus de confiance aux électeurs[1, 2].

En 2014, l'Alliance libérale, un parti politique au Danemark, est devenue la première organisation à utiliser la blockchain pour voter.

Depuis octobre 2016, le Parlement européen étudie la possibilité d'utiliser la blockchain pour le vote. Un document[3] rédigé par Philip Boucher, analyste au Parlement européen, appelé « What if Blockchain Technology Revolutionised Voting ? » pose un regard sur la blockchain et le vote électronique.

Philip Boucher se demande si en matière de sécurité et de transparence, la blockchain est la révolution nécessaire pour permettre le vote électronique et, dans l'affirmative, quelles sont les implications pour l'avenir de la démocratie. En réalité, malgré la numérisation de plusieurs aspects importants de la vie moderne, les élections sont encore en grande partie réalisées hors ligne, sur papier. Depuis le début du siècle, le vote électronique a été considéré comme un développement prometteur et (éventuellement) inévitable, qui pourrait accélérer, simplifier et réduire le coût des élections et pourrait même conduire à une plus forte participation électorale et au développement de

1. http://www.blockchaindailynews.com/La-blockchain-promesse-de-lendemains-radieux-pour-la-democratie_a24726.html
2. Par ailleurs, dans un article paru sur Cryptos.net (http://www.cryptos.net/technologie-block-chain-lavenir-democratie-numerique/), on pouvait lire : « En 2012, lors des dernières élections aux États-Unis, une inscription sur huit était invalide ou incorrecte ; tandis que seulement 2,7 millions d'électeurs se sont inscrits dans différents États du pays. Ces statistiques sont terribles pour un système qui est utilisé dans le but de déterminer l'avenir d'une nation, surtout pour un pays aussi puissant que les États-Unis. »
3. http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2016)581918

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

démocraties plus fortes. Aujourd'hui, nous pouvons continuer de faire confiance aux autorités centrales pour gérer les élections ou bien utiliser la technologie blockchain pour distribuer un registre de vote ouvert parmi les citoyens.

Ce document va lancer le débat au sein de la Communauté européenne.

Belem et Voatz, deux solutions innovantes

En matière de vote *via* la blockchain, Belem, une start-up française, propose une solution déjà éprouvée[1] : « La force d'innovation du vote dans la blockchain repose sur le fait que l'enregistrement des votes ne relève plus d'une autorité centralisée mais d'une relation *peer-to-peer*, ce qui assure une parfaite transparence du vote. »

Voici les avantages de la solution Vote by Belem[2] :

- confiance : participer directement au débat public sans s'en remettre à la confiance d'un tiers. Voter devient ainsi un acte absolument démocratique ;
- sécurité : les votes sont enregistrés dans un registre infalsifiable ;
- transparence : les participants peuvent s'assurer que leur vote a bien été pris en compte ;
- simplicité : votez en deux minutes grâce à cette solution intuitive et accessible en permanence.

De son côté, la start-up américaine Voatz[3] permet aux citoyens de voter en toute sécurité à l'occasion de toutes sortes d'élections ou de scrutins *via* un smartphone. Les tentatives antérieures de vote par Internet ont échoué en raison de préoccupations fondamentales autour de la sécurité, de la vé-

1. http://www.frenchweb.fr/voter-via-la-blockchain-experimentations-et-retours-dexperience/240683
2. http://vote.belem.io/
3. https://voatz.nimsim.com/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

rification et de l'anonymat de vote. Avec Voatz, en utilisant la sécurité biométrique avancée et la technologie blockchain pour l'irréfutabilité, il est possible de relever tous les défis et de rationaliser considérablement le processus de vote et de vérification de l'identité.

Propriété intellectuelle

Et puisque nous en étions à citer Belem, poursuivons avec elle et découvrons comment elle ouvre la voie d'un nouveau marché notarial. Belem a mis au point un module d'authentification qui offre un moyen simple, économique et sûr de consigner et protéger des données personnelles ou professionnelles.

La blockchain permet d'enregistrer une preuve datée, irréfutable et non modifiable de l'existence d'une donnée ou d'un document, l'horodatage de celle-ci *via* sa signature numérique fonctionnant comme la preuve de son existence à une date précise.

Ainsi le contenu de la donnée répertoriée peut être partagé ou rester confidentiel, mais l'empreinte de la donnée est auditable par tous. La sécurité de la donnée est quant à elle assurée. L'inviolabilité de la blockchain contrecarre la vulnérabilité des structures notariales actuelles.

Le module d'authentification de Belem permet aussi bien d'attribuer l'origine d'un brevet industriel ou d'une idée que d'enregistrer des certificats de naissance/décès, des preuves de résidence et de solvabilité, des données de marchés financiers, ainsi que de digitaliser des diplômes, des titres de propriété fonciers ou physiques (clé, voitures, œuvres d'art, actions et obligations, etc).

Voilà donc un autre exemple concret d'usages réalisés ou réalisables *via* la technologie blockchain.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Analyse de données

Poursuivons avec Belem qui développe une application très intéressante : « Après avoir sondé la force disruptive de la blockchain dans le champ de la démocratie participative et de la propriété intellectuelle, nous nous consacrons au développement d'une plateforme innovante, qui permet d'analyser des données confidentielles sans compromettre le caractère privé des informations transmises, tout en maintenant un niveau de confiance maximal. »

Ainsi le champ d'application de la plateforme est vaste : finance, assurance, santé, e-commerce, Internet des objets, etc. Enfin, il regroupe tous les domaines dans lesquels des parties souhaitent analyser des données sans les révéler.

Supply chain/*logistique*

Mais ce tour d'horizon ne serait pas complet si nous ne présentions pas les projets dans le domaine très prometteur de la *supply chain*. Voilà bien un domaine où la technologie blockchain devrait exceller car c'est un secteur dans lequel il y a de nombreux intervenants, des documents à valider, des paiements à effectuer et de nombreuses authentifications et processus à réaliser.

La plupart des produits que nous achetons ne sont pas faits par une seule entité, mais par une chaîne de fournisseurs qui vendent leurs composants (par exemple, du plastique pour les emballages) à une entreprise qui assemble et commercialise le produit final. Que l'un de ces composants manque ou que l'un des participants ne respecte pas la procédure et c'est la chaîne qui s'en trouve brisée.

Que se passerait-il si une entreprise pouvait fournir de façon proactive des enregistrements numériques permanents et auditables qui montreraient aux parties prenantes l'état

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

d'avancement du produit à chaque étape de son acheminement ? C'est une des nombreuses idées d'application de la technologie blockchain dans la *supply chain*.

Kuovola Innovation

La start-up finlandaise Kuovola Innovation[1] travaille sur une solution blockchain qui permet l'adjudication intelligente à travers la chaîne d'approvisionnement. Les palettes équipées d'étiquettes RFID défilent et publient leurs besoins en passant du point A au point B du registre partagé. Les applications minières des transporteurs engagent ensuite des enchères pour emporter le marché. La RFID attribue alors le travail au soumissionnaire avec les conditions les plus appropriées et la transaction est enregistrée sur la blockchain. Enfin l'expédition est progressivement suivie dans la chaîne d'approvisionnement.

La révolution de la blockchain des données

La technologie blockchain porte la promesse de l'enregistrement inaltérable de transactions, de preuves d'existence de données, voire de programmes et de leurs données associées. Les deux plus importantes chaînes en utilisation, celles de Bitcoin et d'Ethereum, permettent ces fonctionnalités à des degrés divers. Il est aujourd'hui bien compris que seules la preuve de travail et la rémunération des mineurs garantissent cette inaltérabilité. Plus intéressant encore, elles permettent l'enregistrement inaltérable pour un coût fixe initial, la maintenance étant obtenue par l'empilement de calculs gigantesques, progressivement inaccessibles à toute tentative d'attaque. Cela est vrai quel que soit le futur : que le réseau de mineurs persiste ou s'arrête.

1. http://www.kinno.fi/en

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

La preuve d'existence de données est obtenue par le calcul de sommes cryptographiques à partir des fichiers. Cette opération est simple. Mais rendre probante une interaction sophistiquée comportant de nombreux documents, signatures, certificats d'horodatage requiert de lier les données, leurs sommes de contrôle, signatures et certificats d'horodatage.

Une technologie révolutionnaire, qui pourrait être qualifiée de « blockchain des données », permet d'embarquer dans tout fichier, de quasiment tout format, des preuves d'intégrité, clés publiques, signatures numériques, liens cryptographiques vers d'autres documents et toutes autres métadonnées librement pour l'utilisateur.

Cette solution, protégée par des brevets internationaux d'origine française, est portée par la société KeeeX[1], une start-up française. La preuve d'intégrité du fichier est promue en une identité, son « identifiant » : un nom unique, humanisé mais artificiel, accessible aux moteurs de recherche dans tout document, et utilisable dans tout autre document ou fichier pour le désigner.

Un des effets techniques de la solution KeeeX est que les données ainsi équipées sont réputées intègres et signées pour l'éternité, avec leurs connexions, sans possibilité de corruption, car aucune attaque n'est connue sur les *hashes* cryptographiques utilisés : il est impossible de créer deux fichiers ayant la même « identité », encore moins de forger un fichier ayant le même identifiant qu'un autre déjà connu. Il est ainsi possible de déployer des données et de rendre des processus métier probants, qu'ils soient automatisés ou humains, sans devoir mettre en place une infrastructure complémentaire à l'existant.

1. KeeeX, solutions de confiance blockchain : https://keeex.me/fr/

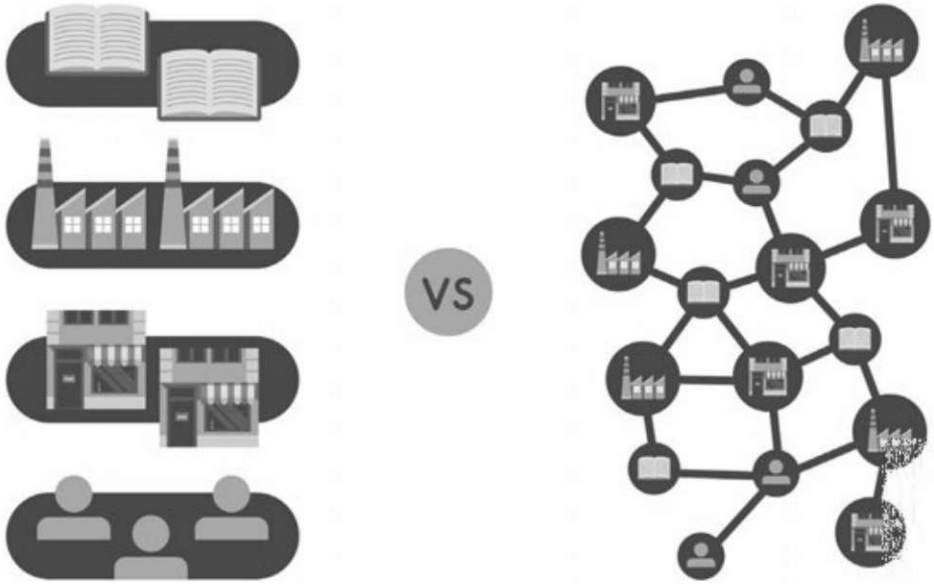
Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Bien sûr, l'identifiant d'un fichier trouve naturellement sa place dans une transaction enregistrée dans la blockchain. On génère ainsi une continuité de confiance et de preuve de la blockchain jusqu'aux données et fichiers seuls. La combinaison de Bitcoin et de KeeeX donne ainsi pour la première fois dans l'histoire des données plus de valeur probante à un document numérique qu'à un original papier.

Cette révolution du document probant autoportée a des applications dans tous les secteurs de l'information et de l'industrie : contrats et processus contractuels avec multi-signature et multi-date, photographies probantes et datées, factures certifiées, feuilles de paie certifiées, notes de frais certifiées, diplômes et bulletins de notes certifiés, recommandés avec accusé de réception, identités numériques et processus de connaissance du consommateur pour n'en citer que quelques-uns.

Éducation



De nombreux projets émergent dans le monde de l'éducation car après l'enseignement à distance voici venue la possibilité d'échanger, de valider des cours ou des devoirs et bien plus encore.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Ainsi une récente étude de KnowledgeWorks[1] a exploré le potentiel de la technologie blockchain au niveau des écoles, des enseignants, des parents et des élèves en ce qui concerne l'avenir de l'apprentissage.

Un organisme sans but lucratif, BEN[2] ou Blockchain Education Network, vaste réseau international pour et par les étudiants, a été fondé en 2014 afin de créer des clubs Bitcoin et blockchain sur leurs campus universitaires. En explorant cette expérience socio-économique en toute sécurité avec leurs pairs, les élèves construisent de nouveaux usages et des innovations. Au total, l'effort combiné de tous ces clubs crée un riche réseau de blockchains interconnectées à travers le monde pour partager des ressources et explorer de nouveaux usages.

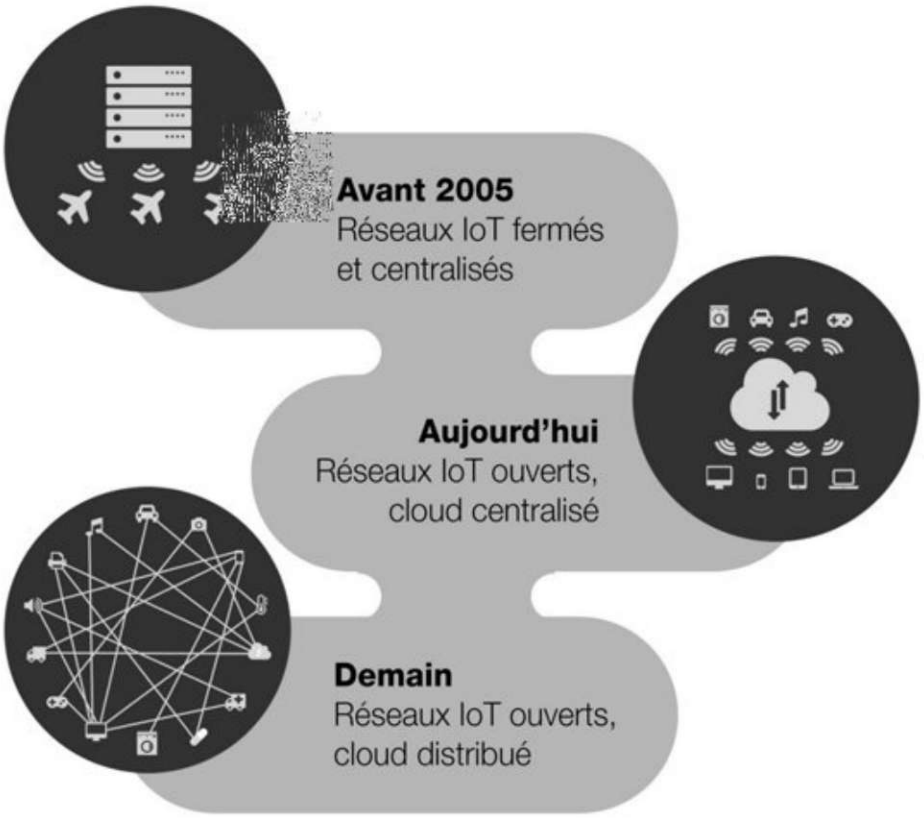
Autre exemple, l'école Holburton de San Francisco, une école de développement de logiciels, utilise la technologie blockchain pour stocker et délivrer ses diplômes. Le cryptage et l'authentification à deux facteurs sont utilisés pour créer, signer et placer le diplôme dans la base de données de la blockchain. L'école fournit toujours aux élèves des copies papier, mais un numéro de compensation décentralisée (DCN) créé par le système est généré, ce qui permet l'authentification par les futurs employeurs.

1. Learning on the block : http://www.knowledgeworks.org/learning-block-smart-transactional-models D'après l'étude : « Il est important pour les éducateurs et les autres parties prenantes de réfléchir à tous les impacts possibles, tant positifs que négatifs, que la blockchain pourrait avoir sur l'avenir de l'apprentissage. […] Du suivi des absences à la gestion des délais des devoirs, les nouvelles technologies sont souvent tournées vers la résolution d'un problème dans une école ou une classe. Mais, si au lieu de résoudre un problème, la technologie permettait d'ouvrir des portes pour l'apprentissage ? »
2. https://blockchainedu.org/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

La blockchain est réellement une technologie de désintermédiation qui a des applications multiples dans le monde de l'apprentissage au niveau individuel, institutionnel, de groupe, national et international et dans toutes sortes de contextes : écoles, collèges, universités, MOOC, entreprises, apprentissages et bases de connaissances.

Internet des objets



L'UIT[1] (Union internationale des télécommunications) définit l'Internet des objets (IoT) comme une « infrastructure mondiale pour la société de l'information, qui permet de disposer

1. UIT : Organisation des Nations unies pour les télécommunications. Fondée en 1865, elle compte quelque 180 pays membres. Son rôle est d'harmoniser le développement des télécommunications dans le monde. Le siège de l'UIT est à Genève.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution ».

Nous pourrions ajouter que les objets qui composent ce monde de l'IoT ne font pas que simplement dialoguer entre eux mais sont aussi capables d'interagir et surtout d'engager entre eux des contrats et des microtransactions de façon sécurisée.

L'infrastructure de confiance algorithmique distribuée de la technologie blockchain va idéalement servir les besoins de l'IoT, et les technologies naissantes comme IOTA ou beAchain (solution française) devraient permettre de très nombreuses applications concrètes.

L'analyse de Xavier Dalloz

« Avec l'Internet des objets, le protocole blockchain va trouver l'une de ses plus larges applications, compte tenu des problèmes colossaux de confiance qui ne manqueront pas de se poser... la technologie blockchain va devenir l'infrastructure d'un monde globalement numérique et massivement interconnecté avec notamment le Wearable Computing, l'IoT, les capteurs, les smartphones, les ordinateurs portables, les appareils du quantified self, le Smarthome, le Smartcar et le SmartCity[1]. »

Blockchain et entreprises, une opportunité à saisir

Si l'on raisonne à partir du postulat que la technologie blockchain est disruptive car elle va perturber plus ou moins fortement l'entreprise et son modèle, alors elle peut être

1. Dirigeant du cabinet de conseil Xavier Dalloz Consulting spécialisé dans le suivi des technologies de l'information, http://www.dalloz.com/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

perçue comme une menace ; si au contraire, on admet que la blockchain peut fluidifier les processus et les réseaux, améliorer les relations clients et fournisseurs, accélérer les flux financiers tout en diminuant leurs coûts (entre autres gains et avantages) alors, elle représente une opportunité.

La blockchain, une technologie disruptive bénéfique pour les entreprises

À l'instar des Fintech[1] qui bousculent, voire disruptent, le paysage bancaire et financier, la blockchain mais aussi les blocktech[2] pourraient à leur tour, mais d'une façon plus globale, disrupter l'ensemble des organisations.

Sur les marchés les entreprises se livrent une bataille pour créer de la valeur dans un environnement en constante évolution. Du protocole TCP-IP au Web communautaire, en passant par les smartphones, l'e-commerce et les réseaux sociaux, les révolutions technologiques des dernières décennies ont rebattu les cartes et creusé le fossé numérique qui sépare certaines entreprises d'une même industrie.

Celles qui n'ont pas su s'adapter en ont payé le prix fort (Microsoft et le virage du mobile) ou ont tout simplement disparu (Kodak et le numérique). Dans cet environnement innovant et instable, identifier les évolutions technologiques le plus en amont est un enjeu majeur.

Anticiper la possible disruption totale ou partielle de sa propre activité, que l'on soit dans le commerce, dans l'assurance ou

1. Organisation qui utilise les technologies financières innovantes pour fournir ou soutenir des services financiers.
2. Organisation qui utilise les technologies blockchain : France Blocktech, http://www.franceblocktech.org

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

dans toute autre activité, c'est anticiper ou observer les cas d'usage qui apparaissent dans son industrie et surtout ébaucher des solutions blockchain afin d'éviter une disruption partielle ou totale de son propre modèle économique du fait de concurrents plus rapides sur le sujet de la transformation numérique ou de blocktech plus agiles.

Ainsi, après avoir identifié les principes de la technologie blockchain et ses impacts possibles sur votre métier, posez-vous pêle-mêle quelques questions :

- Quels sont les processus au cœur de votre métier impactés ou susceptibles d'être impactés par la technologie blockchain ?
- Quels sont les risques et les opportunités par rapport à votre modèle d'affaires ?
- Quels sont les axes prioritaires en matière de risques et d'opportunités ?
- Qui seront les nœuds (participants) de cette blockchain ?
- Quel est le consensus envisagé et les types d'autorisations que vous souhaitez configurer dans votre expérience blockchain ?
- Quels sont les coûts, délais et contraintes pour cette mise en œuvre ?
- Quels sont les risques liés à cette mise en œuvre ? Quels en sont les impacts possibles ?
- Comment allez-vous organiser un test blockchain (PoC)[1] ? Et sur quel(s) processus ?
- Possédez-vous les compétences techniques en interne ou devez-vous externaliser tout ou partie de cette mise en œuvre ?

1. PoC (*proof of concept* ou preuve de concept) est une démonstration de faisabilité, une réalisation courte ou incomplète d'une certaine méthode ou idée pour démontrer sa faisabilité. C'est une étape importante pour aboutir à un prototype pleinement fonctionnel.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

- Avez-vous les ressources internes pour mener ces diagnostics et ces études ?
- Votre organisation professionnelle ou vos confrères travaillent-ils sur ces sujets ?
- Ne pourriez-vous pas mutualiser tout ou partie de ces travaux afin d'optimiser les résultats et diminuer les coûts associés ?
- Existe-t-il une organisation ou un syndicat professionnel dédié blockchain qui pourrait vous apporter aides et concours avant, pendant et après ce projet ?

Bien évidemment cette liste n'est pas exhaustive et les questions varieront en fonction de l'entreprise, de son business model, de son niveau de transformation numérique, etc.

Les entreprises qui adoptent la technologie blockchain peuvent réduire leurs coûts, augmenter la résilience et la sécurité de leurs bases de données, optimiser et accélérer les échanges avec les tiers, adopter des paiements instantanés à des coûts faibles, proposer de nouveaux services, etc.

Elles peuvent également améliorer et fluidifier leur fonctionnement interne, leurs processus, leurs cycles clients et fournisseurs. En résumé elles peuvent s'auto-transformer et tout ou partie en « chaîne de valeur ».

Qu'est-ce qu'un bon cas d'usage « blockchain de consortium » ?

Aujourd'hui, dans tous les départements innovation des grands comptes, une effervescence, voire une FOMO[1], règne sur la thématique de la blockchain et son cortège annoncé d'implications technologiques, organisationnelles, financières, etc.

1. FOMO, acronyme de l'anglais Fear Of Missing Out (peur de manquer quelque chose).

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Au vu de l'ampleur du changement de paradigme qui se prépare, tout le monde se doit d'identifier les impacts potentiels de la blockchain sur ses métiers.

Nous allons tenter de partager avec vous quelques réflexions nécessaires quand nous cherchons à identifier un cas d'usage pour une première expérimentation autour de cette approche blockchain.

Étant donné que tout ce qui peut se développer en approche blockchain décentralisée peut également être implémenté en approche classique (centralisée), il faut absolument trouver des cas d'usage qui exploitent au maximum les apports et les spécificités de cette technologie. C'est ce que nous avions approché plus haut (voir « Cas d'usage, applications »).

Préambule

Nous parlons bien dans cet exemple de « protocoles de registres distribués » ou « protocoles de consensus distribués », que nous nommerons par abus de langage « blockchain ».

Ensuite, il s'agit ici de la mise en place de « blockchain de consortium », souvent nommée « privée » même si nous préférons le terme « *permissioned* » et non pas de la mise en place d'un cas d'usage pour la mise en œuvre d'une blockchain ouverte (paiement Bitcoin, certification de données, etc.).

Quelle question se poser ?

Le premier réflexe pour tout le monde est d'approcher le sujet par la question : « Quel problème allons-nous résoudre avec la blockchain ? »

Bien que juste, cette approche est toutefois inadaptée car, en ce qui concerne la blockchain, nous traitons d'une technologie de rupture. C'est pourquoi, quitte à adopter une technologie

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

disruptive, alors disruptons notre propre raisonnement et adoptons le Lean Startup[1]. Cette méthode repose sur la vérification de la validité des concepts, l'expérimentation scientifique et le design itératif (méthode agile[2]). En règle générale, elle permet de réduire les cycles de commercialisation des produits, de mesurer régulièrement les progrès réalisés, et d'obtenir des retours de la part des utilisateurs. Elle permet également de concevoir des produits et des services qui satisfont au mieux la demande des consommateurs, avec un investissement initial minimal.

C'est cette méthode que nous proposons d'adopter pour notre cas d'usage. Et étant donné que le paradigme est nouveau, une meilleure façon d'approcher le sujet est plutôt de se poser la question suivante : « Quelle nouvelle opportunité (marché, service, écosystème) allons-nous pouvoir créer avec une approche blockchain ? »

Les caractéristiques d'un bon cas d'usage blockchain

Une fois cette question posée, il faut trouver un sujet, une nouvelle opportunité, qui rassemble plusieurs caractéristiques qui utilisent au mieux les apports des registres distribués ouverts ou fermés.

Pour un cas d'usage en entreprise, nous avons recensé huit caractéristiques à combiner pour constituer un cas d'usage intéressant :

- il faut tout d'abord un *besoin de stockage de données*. Cet aspect est complètement évident car nous parlons d'un registre distribué ;

1. Lean Startup : concept développé en 2008 par Eric Ries sur la base de la pensée Lean dans des entreprises high-tech de la Silicon Valley. Cette approche repose sur la vérification de la validité des concepts, l'expérimentation scientifique et le design itératif. Elle permet de réduire les cycles de commercialisation des produits, de mesurer régulièrement les progrès réalisés, et d'obtenir des retours de la part des utilisateurs.
2. Certains consultants de la start-up Blockness (voir acteurs en fin d'ouvrage) sont très actifs sur ce sujet.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

- avec de *multiples participants en écriture*. Si dans notre cas d'usage, il n'y a qu'un seul acteur qui écrit des données, notre blockchain n'a pas d'intérêt. Une blockchain est un système qui fait intervenir plusieurs acteurs en écriture, éventuellement sur les mêmes données. À ce stade, les bases de données traditionnelles ne sont pas encore à éliminer car elles permettent également d'avoir plusieurs utilisateurs en écriture ;
- avec des *participants qui ont des intérêts divergents ou une absence de confiance*. À noter que les intérêts divergents ou l'absence de confiance ne signifie pas que ce sont des entités différentes. Ainsi deux départements d'une même société peuvent fonctionner avec différentes règles et visions de la réalité qui font que les données d'un département ne font pas foi par rapport aux règles et aux activités de l'autre département (exemple : la logistique et la comptabilité n'utilisent pas forcément les même règles et statistiques) ;
- avec une *volonté ou nécessité de ne pas passer par un tiers de confiance ou un GIE*. Si on s'arrêtait là, il y a une solution évidente au problème posé qui est de fonctionner par le biais d'un intermédiaire de confiance ou d'une GIE dont la neutralité permettra de fonctionner en toute confiance. Pour mettre en œuvre une blockchain, il est important que les différents acteurs aient une volonté commune de ne se fier à aucun intermédiaire de confiance, mais de mettre en œuvre un registre distribué dont chacun est un participant. Parmi les bonnes raisons qui justifient de ne pas vouloir passer par un intermédiaire de confiance, on peut citer : la réduction des coûts de transaction, des transactions plus rapides, une réconciliation comptable automatisée… ou simplement l'incapacité des acteurs à trouver le bon intermédiaire de confiance ;

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

- un *besoin de règles qui contrôle les transactions*. Il est important de déterminer les règles qui vont permettre de valider les transactions et ces règles seront à implémenter au niveau de l'algorithme de consensus de la blockchain. Sans la capacité de définir ces règles, la technologie blockchain ne pourra pas fonctionner ;
- une *capacité de déterminer qui sont les validateurs*. Dans une blockchain, il y a des nœuds validateurs (souvent appelés « mineurs ») qui participent au consensus distribué et ces nœuds ont un rôle essentiel et le pouvoir de censurer les transactions jugées malicieuses ou d'arbitrer les transactions en conflit. Il faut donc choisir avec intelligence les différents participants afin d'établir un équilibre des pouvoirs entre les différents acteurs ;
- une *interaction transactionnelle*. Il faut également que l'interaction entre les participants soit de nature transactionnelle comme par exemple lorsqu'il s'agit d'un actif qui change de propriétaire ou de gestionnaire (exemple : *supply chain*) ;
- avoir *un garant de la contrepartie de l'actif modélisé*. Enfin, la blockchain va modéliser des interactions et des transactions entre ces participants. Il est nécessaire que les entreprises apportent des garanties au regard de l'actif qui sera modélisé (marchandises, actifs, etc.), sinon la réalité de la blockchain sera en conflit avec le terrain.

Synthèse

Il faut raisonner de la façon suivante : « Quelle opportunité allons-nous créer avec la blockchain ? »

Il est nécessaire que les participants à la blockchain aient une bonne raison de ne pas vouloir mettre en œuvre un tiers de confiance centralisateur.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Bien évidemment, notre propos n'est pas de vous expliquer en une page ou deux ce que cette méthode Lean Startup implique en amont et en aval du projet initié mais simplement de brièvement tenter de vous démontrer que vous pourrez tirer un grand profit, tant en matière de timing, d'organisation et de gains financiers, de cette approche par le *proof of concept* que vous souhaitez développer.

Avec cette méthode, on ne cherche pas un problème à résoudre et on ne part pas de la technologie mais du besoin réel, estimé lors des séances préalables de brainstorming.

En conclusion, la blockchain est un levier pour innover et créer de nouveaux services ou produits, de nouvelles opportunités.

Quelle technologie adopter ?

Pour votre projet, devez-vous opter pour une blockchain ou une base de données partagée ?

Nous ne reviendrons pas en détail sur le thème blockchains publiques *versus* blockchains privées, mais nous avons expliqué qu'une blockchain publique (Bitcoin, Ethereum, etc.) est ouverte à tout participant qui peut valider des transactions et participer au consensus et qu'une blockchain privée intègre nativement un contrôle d'accès – cela implique que chaque participant ou nœud du réseau exerce un contrôle sur les entrants dans ce réseau ainsi que sur les participants au consensus de la blockchain.

Ainsi une blockchain privée permet aux institutions financières de maintenir une base de données partagée et structurellement cohérente des transactions. Cela permet à chaque institution participante de lire les données du grand livre distribué avec la garantie qu'il est valide et réconcilié avec les données détenues par les autres institutions participantes.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

La sécurité d'une blockchain publique, comme Bitcoin par exemple, provient de son consensus ou de sa preuve de travail (*proof of work*) ou minage, ce qui rend mathématiquement impossible de fausses transactions ou écritures et surtout rend impossible la modification ou l'effacement de ces enregistrements. De plus, dans une blockchain publique, l'utilisation de la cryptographie et des structures de données telles que les arbres de Merkle permettent de vérifier que les transactions non valides ne sont pas ajoutées à la blockchain.

Avec les blockchains publiques, la confiance vient plus du processus lui-même que du statut d'un participant. Dans cette base de données partagée et sécurisée, les participants ont leurs propres copies des données stockées… Les paiements sont validés de façon collective par les participants et mis à jour à travers le réseau presque immédiatement. La cryptographie assure que les transactions ne peuvent être engagées que par des parties certifiées et qu'il n'y a qu'une version de la vérité.

À partir de ces remarques générales sur les blockchains privées et publiques, on peut se demander si les blockchains privées ne seraient pas, tout simplement, un nouveau type de base de données.

La question semble légitime eu égard au fait qu'une base de données peut être directement partagée sans nécessairement exiger la présence d'un administrateur central, d'un tiers de confiance. Cela contraste avec les bases de données types SQL, par exemple, qui sont contrôlées par une seule entité – quand bien même nous pouvons y observer une architecture distribuée.

De leur côté, les blockchains offrent indéniablement la confiance, la robustesse et par conséquent une plus grande sécurité de l'information. Donc, si dans votre projet, la confiance et la robustesse ne sont pas une priorité, alors une base de données

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

partagée peut faire l'affaire. En revanche, si vous recherchez une totale désintermédiation (suppression d'une autorité centrale), alors il vous faudra choisir une technologie blockchain.

Les questions à se poser

Comme nous l'avons vu précédemment dans notre exemple de cas d'usage, imaginons que nous devons aborder la question d'un choix parmi ces technologies et ainsi déterminer le consensus et les types d'autorisations que nous souhaiterions configurer dans notre expérience blockchain. Nous devons répondre à ces quelques questions :

- Qui sommes-nous ?
- Que voulons-nous atteindre ?
- Qui seront les nœuds ?
- La confidentialité est-elle primordiale ?
- Avons-nous besoin d'identifier des provenances ?
- Avons-nous besoin d'horodater ?

Si nous poussons un peu plus loin le raisonnement, même un contrat intelligent, qui n'est qu'un « simple bout de code informatique », peut fort bien être inséré dans une base de données partagée et y jouer son rôle à la perfection. Nous pourrions simplifier en disant que tout est question d'algorithmes et de langages. Par opposition, quid d'un contrat intelligent dans une blockchain quand il doit interagir avec l'extérieur ?

Un autre aspect est à prendre en compte : la performance. En effet, aujourd'hui, une blockchain publique sera toujours plus lente qu'une base de données partagée (à pondérer suivant l'usage recherché). Cette lenteur est due aux tâches que la blockchain doit réaliser telles que le mécanisme de consensus

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

ou la génération et la vérification des signatures numériques des transactions. (Mais là aussi nous pourrions nuancer en notant que certaines blockchains privées, grâce à leur architecture et leur consensus, ou certaines blockchains publiques, grâce à de nouveaux algorithmes, offrent d'excellents temps de réponse, sans parler de systèmes hybrides.)

Donc, si vous avez un projet blockchain, et en l'état actuel des technologies, retenez simplement qu'il est important de placer dans la balance les avantages et les inconvénients liés à l'usage que vous pourriez avoir d'une blockchain (publique ou privée), d'une base de données partagée, voire d'une plateforme ou architecture hybride.

En matière de projet blockchain, il n'y a pas de réponse universelle, car chaque organisation, et par voie de conséquence chaque projet, est unique.

Gouvernance et droit

La blockchain fait l'objet d'un très fort intérêt depuis quelques mois. Articles, colloques, présentations sur cette technologie de rupture font florès. Les banques s'y intéressent de très près, conscientes de l'enjeu de celle-ci pour leurs activités et du risque qu'elle peut faire peser sur leurs revenus.

Les banques centrales ne sont pas parmi les dernières à s'y pencher, et même les gouvernements regardent de près les conséquences que cette technologie peut avoir sur les finances publiques et leur souveraineté.

Si les effets économiques de cette technologie semblent de plus en plus évidents, ses conséquences juridiques restent mal définies. Ou plus exactement, la manière dont la loi traite de la blockchain reste floue.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Deux grandes questions se posent à cet égard : une première sur la gouvernance de la blockchain, et une seconde sur la force juridique des opérations effectuées *via* cette technologie. Dans un cas comme dans l'autre, l'analyse dépend du type d'organisation de la « chaîne », selon que l'on se situe dans une blockchain ouverte ou dans une blockchain fermée. Mais toute analyse sur la question doit garder à l'esprit que la blockchain est avant tout une technologie.

L'analyse de maître Hubert de Vauplane

« Les règles de fonctionnement de la blockchain dépendent de son degré d'ouverture : plus la chaîne est ouverte, moins il y a de gouvernance, et inversement.

Ainsi, dans une blockchain privée, comme celle d'un système de règlement/livraison, ou d'un registre de cadastre, la gouvernance est régie par l'institution qui gère la chaîne : sont ainsi déterminés dans des règlements les conditions d'accès, le fonctionnement, la sécurité, et le mécanisme de reconnaissance légale des transactions.

Inversement, dans la blockchain publique où l'accès est totalement libre, il n'existe pas d'autres règles de fonctionnement que la technologie elle-même (selon l'expression, "*Code is Law*[1]" du juriste américain Lawrence Lessig). La question se pose cependant de savoir si, tout comme l'Internet, une certaine gouvernance n'est pas nécessaire. »

Qu'est-ce qu'un logiciel libre ?

Dans le monde du logiciel, il convient de distinguer les logiciels ouverts (libres) de ceux qui sont protégés par des droits de propriété.

1. Lawrence Lessig (juriste américain), « Code is law, On Liberty in Cyberspace », *Harvard magazine*, janvier 2000, http://harvardmagazine.com/2000/01/code-is-law-html

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Un logiciel est libre si et seulement si sa licence garantit les quatre libertés fondamentales :

- la liberté d'utiliser le logiciel ;
- la liberté de copier le logiciel ;
- la liberté d'étudier le logiciel ;
- la liberté de modifier le logiciel et de redistribuer les versions modifiées.

Les deux dernières libertés ne peuvent s'appliquer que si l'on a accès au code source qui est en quelque sorte la recette de fabrication du logiciel.

Qui est propriétaire de la blockchain ?

Là encore, la réponse dépend du type de blockchain utilisée :

- Dans une blockchain privée, la technologie développée par l'organisme en charge de la gestion de la blockchain est protégée par des droits de propriété intellectuelle, même si celle-ci utilise, pour une large partie, les codes sources versés librement lors de la création de la blockchain.
- Inversement, dans la blockchain publique, personne n'est « propriétaire » des codes sources, selon les principes communautaires de la théorie des biens communs.

Cette question de la propriété ou du contrôle des codes sources résonne de manière particulière dans l'industrie financière : il s'agit de la question de la protection des algorithmes utilisés dans certaines transactions financières et développés par des experts (les *quants*) dans la mesure où la plupart de ces algorithmes ne peuvent être protégés par des brevets ou droits d'auteur ; dès lors, ces algorithmes sont gardés secrets.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

La force juridique des opérations réalisées dans la blockchain

La blockchain est une technologie. Certes, totalement nouvelle, mais ce n'est qu'une technologie. Dès lors, les opérations qui s'y traitent soit reflètent des transactions hors de la blockchain (par exemple, les transactions de change ou les ventes d'immeubles et de terrain dans une chaîne privée), soit constituent elles-mêmes des transactions (par exemple, le bitcoin). L'enjeu du développement de la blockchain consiste à savoir comment lier les contrats « crypto » et les contrats « fiat », terme qui regroupe tout ce qui a trait à l'environnement juridique traditionnel[1].

L'analyse de maître Hubert de Vauplane

« C'est le problème de la cyberlaw et plus généralement de la relation entre cryptographie et opposabilité juridique[2]. Dans une blockchain ouverte, les opérations effectuées n'ont pas d'autre force juridique que la valeur que les participants à la chaîne veulent bien leur donner. Ainsi, dans le cas du bitcoin, les échanges de cette crypto-monnaie n'ont pas de valeur légale ; ils ne sont pas reconnus comme opposables aux tiers, mais uniquement entre l'acheteur et le vendeur. En l'absence de gouvernance mondiale de la blockchain publique, il n'en sera pas autrement. La situation est différente dans les chaînes privées. Tout d'abord, ces chaînes ne peuvent fonctionner qu'avec des règles élaborées par l'entité en charge des activités. Ainsi, dans les projets de blockchains relatifs au règlement/livraison d'instruments financiers ou de

1. Pour une explication très complète des aspects juridiques de la blockchain, voir Quinn DuPont et Bill Maurer, « Ledgers and Law in the Blockchain », *The King's Review*, 2015 : http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/
2. Voir l'excellent ouvrage de Jean-François Blanchette, *Burdens of proof, Cryptographic Culture and Evidence Law in the Age of Electronic Documents*, Hardcover, 2012.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

devises, les blocs de la chaîne ne font que refléter des opérations réalisées hors de la chaîne. Dans ce cadre, ces blocs constituent les modalités de règlement et/ou de livraison des opérations d'achat ou de vente de devises ou d'instruments financiers[1]. En conséquence, la chaîne privée fonctionne selon des règles internes opposables aux participants. La situation est la même pour les projets de chaînes privées relatifs au cadastre. Les blocs ne font qu'enregistrer des transactions sans constituer par eux-mêmes les transactions[2]. La chaîne de blocs constitue ici au mieux une preuve de la propriété, preuve qui n'est guère opposable aux tiers sans intervention du législateur pour étendre le régime de la preuve, un peu comme la signature électronique. Certes, dans les chaînes privées locales (comme les cadastres), un État peut légiférer sur la portée de ces blocs et décider que ceux-ci constituent soit des preuves réfragables de propriété, soit des preuves irréfragables, voire le titre de propriété lui-même ! Mais dans la mesure où les opérations de la chaîne publique mais aussi privée dépassent les frontières, les modalités de détermination de ce régime de preuve ne peuvent être élaborées que *via* une convention internationale. À défaut d'accord, on peut craindre la mainmise juridique par une puissance étatique plus forte que les autres sur la chaîne de blocs. Le précédent de l'Internet et la mainmise des États-Unis doit ici servir d'exemple. Le risque de perte de souveraineté constitue un risque réel qui ne peut pas être éludé. »

1. La question de l'utilisation de la blockchain dans les opérations de règlement/livraison dans l'industrie financière illustre les bouleversements que cette technologie peut apporter : un registre décentralisé privé peut demain remplacer les dépositaires centraux tels que Euroclear, DTCC et autres, sous réserve de régler préalablement la question juridique du droit de propriété des titulaires de titres. Voir Pascal Bouvier, « Distributed Ledgers Part II : Clearing, Settlements and Legal frameworks » : http://finiculture.com/distributed-ledgers-part-ii-clearing-settlements-and-legal-frameworks/
2. Il est désormais possible d'enregistrer sur la blockchain la preuve horodatée, irréfutable et indélébile de l'existence d'un document sans avoir à en révéler le contenu. L'expérimentation proposée par *proof of existence* n'intègre évidemment pas le document lui-même dans le registre, mais une simple empreinte qui permet de prouver que le document existait à une époque donnée et qu'il est lié à une adresse précise.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Pourquoi un *smart contract* n'est pas un contrat

« *Code is Law* » est l'une des phrases les plus communément invoquées pour expliquer le fait qu'une transaction, une fois qu'elle a été exécutée sur une blockchain, ne peut plus être modifiée ni altérée par quiconque et cela sans le contrôle d'un organe central. Nous serions ainsi tentés de dire que les programmes écrits pour une blockchain font office de loi car ils s'appliquent automatiquement et les comportements qui y sont décrits sont respectés par construction.

Cette caractéristique propre aux *smart contracts* est en réalité vraie pour tout programme informatique : l'ordinateur exécute aveuglément le code en respectant exactement les instructions qu'on lui donne. La propriété supplémentaire des blockchains est que la base de données étant inaltérable, on ne peut pas modifier son état et notamment les « soldes » des comptes en monnaie virtuelle sans l'accord des propriétaires des adresses. C'est cette dernière propriété qui fait qu'en réalité, « *Code is Law* » est une affirmation fausse du point de vue de la loi telle qu'elle existe dans le droit et qu'un *smart contract* n'est en réalité pas un contrat au sens légal.

En effet, un *smart contract* est écrit par un développeur (un être humain, en tout cas jusqu'à présent) et exécuté par des machines (l'ensemble des nœuds de la blockchain). Si l'exécution du contrat est infaillible car exactement conforme à ses termes (le code), sa rédaction ne l'est pas. L'aventure de The DAO (voir chapitre 2) en est un exemple flagrant. Le contrat passé entre les investisseurs à The DAO et les futurs projets comportait au moins une clause dont l'application stricte a conduit au transfert d'environ 40 millions de dollars selon une modalité qui, si elle était prévue par le contrat (sinon elle n'aurait pas pu s'exécuter), n'avait pas été prévue par les contractants.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

L'article 1108 du Code civil français consacre le principe de la volonté des parties concernant la formation du contrat :

- Les parties ont-elles voulu s'engager ? Il faut vérifier leur *consentement*.
- Étaient-elles aptes à le vouloir ? C'est le problème de leur *capacité*.
- Qu'ont-elles voulu ? Il faut un objet à leur *engagement*.
- Pourquoi l'ont-elles voulu ? L'engagement doit avoir une *cause*.

Ainsi, avons-nous tous réellement la capacité à contracter un engagement rédigé dans un *smart contract* ? La réponse est évidemment non. Il était possible à tout un chacun de se rendre compte de la faille qui résidait dans le *smart contract* de The DAO et de voir que cette clause du contrat n'était pas conforme à l'objet de l'engagement, mais seule une personne s'en est rendu compte et en a profité.

Le second problème concerne la réversibilité et la possibilité de rompre l'engagement. Une fois le transfert prévu par le *smart contract*, mais pas prévu par les contractants, effectué, il a été impossible de revenir simplement à la situation antérieure sans contrevenir aux principes fondamentaux de la blockchain. Dans le cas d'un contrat classique, quand il est avéré que l'une des parties n'était pas en capacité de contracter, le contrat est annulé par un tribunal et ses effets annulés également. Le tribunal force la partie qui a tiré profit de la situation à rembourser la partie lésée, par un moyen de saisie si nécessaire. Cela est impossible sur une blockchain si cela n'a pas été prévu dès la création des contrats. C'est la seconde raison pour laquelle un *smart contract* n'est pas un contrat.

Alors que faire ? À court terme, pour qu'un *smart contract* se rapproche d'un contrat, il est nécessaire, d'une part de le faire

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

rédiger, auditer et valider par une personne en capacité de le faire, et d'autre part de permettre la réversibilité des actions exécutées suite à la signature de ce contrat si un organisme autorisé (un tribunal par exemple) en décide ainsi.

Dans le langage des développeurs, nous parlons de *patterns* à propos de programmes informatiques développés en respectant certains principes définis à l'avance, ou de *frameworks* quand ces programmes réutilisent du code existant et s'exécutent au sein d'un environnement prédéfini, en en respectant les principes de fonctionnement. Il est nécessaire aujourd'hui que des développeurs et des juristes travaillent main dans la main pour créer des *patterns* de *smart contract* et des *frameworks* dont la structure et les caractéristiques respectent le droit de la juridiction dans laquelle ils s'appliquent.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Chapitre 4

La blockchain demain

« Le futur a été créé pour être changé. »

Paulo Coelho

Copyright © 2017 Eyrolles.

Copyright © 2017 Eyrolles.

Révolution en marche

L'économie et la société vont connaître de grands bouleversements, que certains qualifient de disruption, voire de révolution. Quoi qu'il en soit, une profonde mutation va s'opérer sur de très nombreux usages.

Afin de mieux identifier et de cerner cette potentielle révolution, faisons un bref tour d'horizon des précédentes révolutions qui ont impacté nos économies et nos sociétés depuis le XVIIIe siècle.

Les révolutions industrielles

Nous pouvons distinguer cinq âges successifs, dont trois révolutions industrielles de 1771 à nos jours[1].

1771 – La 1re révolution industrielle : l'âge de l'industrie mécanisée et la puissance hydraulique

Lieu d'origine : Grande-Bretagne.

Fait déclencheur : le moulin d'Arkwright ouvre ses portes à Cromford.

Industries nouvelles ou redéfinies : industrie mécanisée du coton, fer forgé, machinerie.

Infrastructures nouvelles ou redéfinies : canaux et voies navigables, puissance hydraulique.

1829 – L'âge de la vapeur et des chemins de fer

Lieu d'origine : Grande-Bretagne.

1. Source : Carlota Perez, « Technological Revolutions and Techno-economic Paradigms », *Technology governance*, janvier 2009 : http://technologygovernance.eu/files/main//2009070708552121.pdf

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Fait déclencheur : test de la machine à vapeur Rocket pour le Liverpool-Manchester.

Industries nouvelles ou redéfinies : moteurs et machines à vapeur, mines de fer et de charbon (rôle central), construction ferroviaire, production de matériel roulant, énergie vapeur pour de nombreuses industries (y compris les textiles).

Infrastructures nouvelles ou redéfinies : chemin de fer, service postal, télégraphe (à l'échelle nationale), grands ports, grands dépôts et grands voiliers, gaz de ville.

1875 – La 2e révolution industrielle : l'âge de l'acier, de l'électricité et de l'ingénierie lourde

Lieu d'origine : Grande-Bretagne, États-Unis et Allemagne.

Fait déclencheur : l'usine d'acier de Carnegie Bessemer ouvre à Pittsburgh, Pennsylvanie.

Industries nouvelles ou redéfinies : acier bon marché, chimie lourde et génie civil, industrie des équipements électriques, cuivre et câbles, aliments en conserve et en bouteille, papier et emballages.

Infrastructures nouvelles ou redéfinies : expéditions dans le monde entier avec des navires à vapeur rapides, canal de Suez, chemins de fer transcontinentaux, grands ponts et tunnels, télégraphe mondial, téléphone (principalement à l'échelle nationale), réseaux électriques (pour l'éclairage et l'utilisation industrielle).

1908 – L'âge du pétrole, de l'automobile et de la production de masse

Lieu d'origine : États-Unis et Allemagne.

Fait déclencheur : le premier modèle T sort de l'usine Ford à Detroit, Michigan.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Industries nouvelles ou redéfinies : production automobile de masse, combustibles pétroliers et pétrole bon marché, pétrochimie (synthétique), moteur à combustion interne pour automobiles, transport, tracteurs, avions, chars de guerre et électricité, appareils électroménagers, produits réfrigérés et surgelés.

Infrastructures nouvelles ou redéfinies : réseaux routiers, autoroutes, ports et aéroports, réseaux de conduits pétroliers, électricité universelle (industrie et habitation), télécommunications analogiques dans le monde entier (téléphone, télex et câblogramme).

1971 – La 3e révolution industrielle : l'âge de l'information et des télécommunications

Lieu d'origine : États-Unis.

Fait déclencheur : le microprocesseur Intel est annoncé à Santa Clara, Californie.

Industries nouvelles ou redéfinies : microélectronique bon marché, ordinateurs, logiciels, télécommunications, instruments de contrôle, biotechnologie assistée par ordinateur et nouveaux matériaux dits « révolutionnaires » (résines, silicones, céramiques).

Infrastructures nouvelles ou redéfinies : télécommunications numériques internationales (câbles, fibres optiques, radio et satellite), Internet, courrier électronique et autres services électroniques, liaisons de transport multimodales à grande vitesse (terre, air, mer). Internet rompt avec les paradigmes habituels de production en augmentant l'intensité des échanges à l'échelle de la planète.

Jeremy Rifkin[1] qualifie ce nouvel âge de l'information et des télécommunications, né en 1971, de « troisième révolution

1. Jeremy Rifkin, essayiste américain, spécialiste de prospective (économique et scientifique). Jeremy Rifkin and the Foundation on Economic Trends : http://www.foet.org/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

industrielle » (ou révolution informatique) qui se distinguerait des secteurs d'activité classiques de la production et aurait démarré avec le développement des nouvelles technologies de l'information et de la communication.

De la révolution informatique au Web 2.0

Nous pourrions résumer les étapes de la période de la « révolution technologique » par :

- l'ordinateur en 1944 ;
- le mainframe en 1954 ;
- le mini-ordinateur en 1964 ;
- l'ordinateur personnel en 1974 ;
- le Macinstosh en 1984 ;
- Internet en 1994 ;
- les réseaux sociaux en 2004 ;
- la blockchain en 2014.

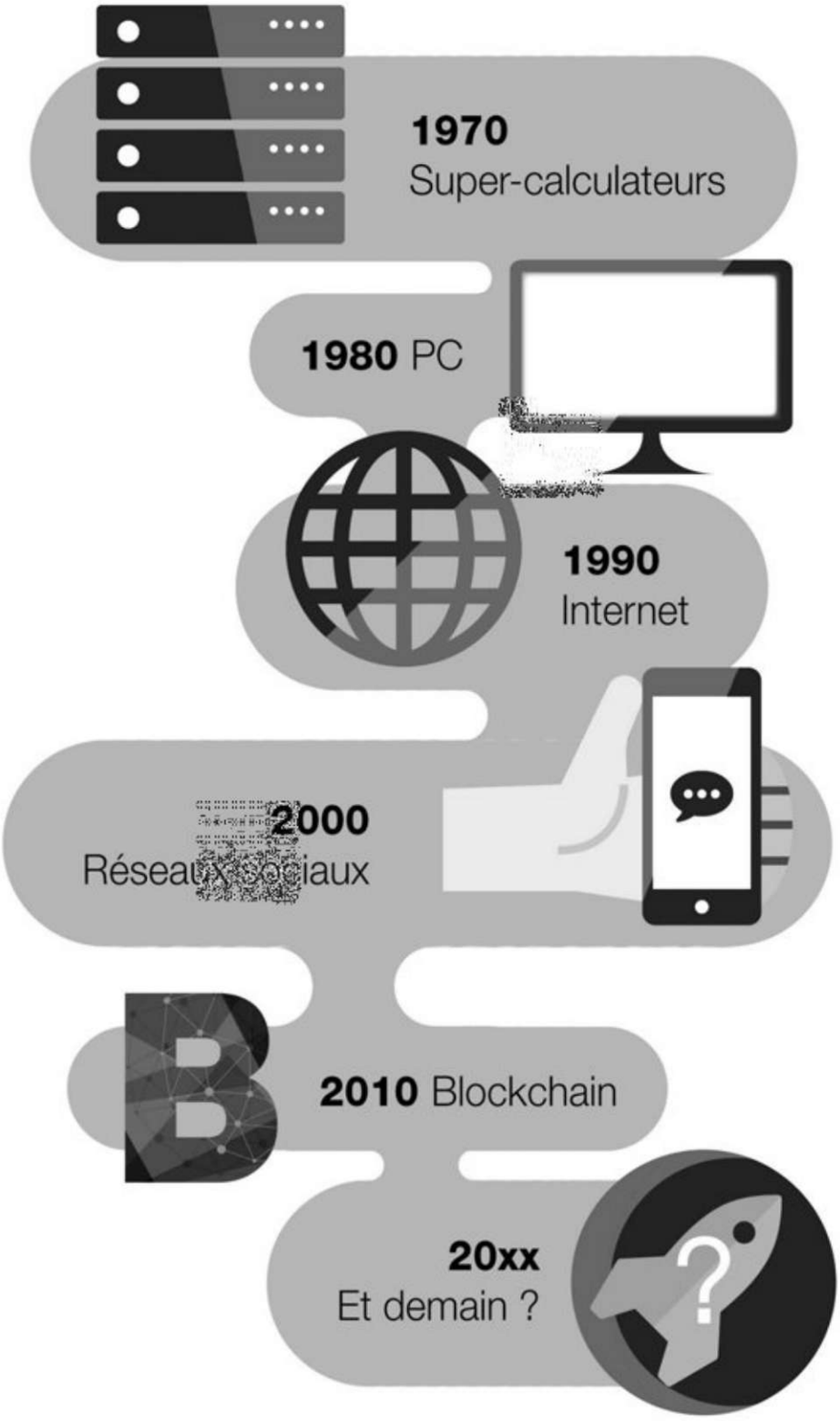
En quoi cette évolution serait-elle une révolution ?

Toujours selon Carlota Perez, ce qui distingue une révolution technologique d'une collection aléatoire de systèmes technologiques et justifie sa conceptualisation comme une révolution sont deux caractéristiques fondamentales :

- les fortes interconnexions et interdépendances des systèmes participants dans leurs technologies et dans leurs marchés ;
- la capacité à transformer profondément le reste de l'économie (et éventuellement la société).

La première caractéristique est la plus visible et définit ce qui est populairement compris comme « la révolution ». Mais, en

Copyright © 2017 Eyrolles.
© Groupe Eyrolles



Copyright © 2017 Eyrolles.
© Groupe Eyrolles

réalité, c'est la seconde caractéristique, la capacité à transformer l'économie et la société, qui justifie vraiment l'usage du terme.

La révolution de la technologie est cette capacité à transformer d'autres industries en de nouvelles industries qui deviennent les moteurs de la croissance sur une longue période tout en entraînant une augmentation généralisée de la productivité dans l'économie accompagnée d'une vaste réorganisation économique et sociétale.

La technologie blockchain serait l'évolution logique de la révolution de l'information démarrée dans les années 1970 par les « mainframes », suivie dans les années 1980 par le PC, les années 1990 par Internet et les années 2000 par les réseaux sociaux. Ces quarante années d'évolution de la technologie et des organisations nous ont conduits aujourd'hui à la technologie blockchain et à sa potentielle disruption.

L'analyse d'Arnaud Péchoux[1]

« En octobre 2015, *The Economist* signe "Le coming out du protocole Blockchain", partagé pour la première fois au-delà des milieux spécialisés et technophiles. Le modèle technologique fondateur du Bitcoin promet de "créer de la confiance" entre des acteurs qui ne se connaissent pas, en excluant le besoin d'organe central ou de tiers de confiance. Cette une a véritablement crédibilisé la promesse et l'a propagée largement. Un an après, l'intérêt reste croissant et l'agitation médiatique s'intensifie autour des possibilités offertes par le protocole.

Force est de constater que cet engagement de confiance prend le contrepied d'un des piliers majeurs de l'économie mondiale. Le marché financier – base de n'importe quel système moderne de gestion d'actifs : assurance, actions, obligations, droit à polluer... – est construit sur la confiance des acteurs entre eux. La promesse d'horizontalisation portée par le protocole blockchain est révolutionnaire.

1. Arnaud Péchoux, société Wavestone : https://www.wavestone.com/fr/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Un des ingrédients du succès d'une révolution est son degré d'attente par la population, le moment où elle surgit et sa facilité à se démocratiser. Dans un contexte mondial de perte de confiance majeure envers les organes politiques et régaliens, les marchés financiers et le système bancaire, le modèle vertical est remis en question sans qu'une proposition de substitut sérieuse n'émerge de cette contestation.

Le mouvement d'ubérisation a lancé l'horizontalisation de secteurs entiers, mais propose un modèle d'intermédiation, en jouant sur l'économie des plateformes ; l'organe centralisateur se rémunère – entre autres – sur la mise en relation. Le report de confiance des institutions centrales vers des communautés d'utilisateurs, grâce aux systèmes de notation, a signé depuis quelques années le premier volet collaboratif de cette transformation des comportements de consommation.

La promesse de la blockchain va plus loin. Elle désintermédie purement et simplement les tiers de confiance. Au moins dans son modèle théorique, le protocole a de quoi inquiéter les organismes centraux. Elle vise le seul profit privé du consommateur final en décentralisant les organes de contrôle. Rappelons que le protocole Blockchain (et le Bitcoin) se base sur une technologie *open source*, et qu'à ce titre, la communauté s'inspire de l'éthique "hacker". La confiance s'appuie sur la technologie. La technologie crée la confiance. Ce point de vue extrême peut être perçu comme effrayant, par le clivage qu'il induit entre les individus participant au mouvement... et les autres.

Survient alors un thème central, inextricable de la blockchain : sa régulation, ses valeurs, sa gouvernance. Le protocole met en réseau des individus, il crée de fait des influences, des forces et mécaniquement une forme de politique. L'alignement des actions directrices de ce système d'information décentralisé, ouvert et transparent, est assurément un enjeu majeur pour le développement, à grande échelle, de la "Machine à consensus". Ici, la feuille est quasiment vierge et toutes les possibilités sont ouvertes : d'un système discriminant et rigide à une organisation mutualiste libertaire, tout peut être envisagé. L'avantage de la période actuelle est que tout peut être expérimenté – et ce, pour en tirer les meilleurs modèles. Ces nouveaux modes doivent être éprouvés dès maintenant, après il sera trop tard...

La survie du protocole passe par des phases de lobbying intenses, la création de mécanismes redistributifs et la mise en place de contre-pouvoirs. Cette page reste à écrire. »

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

D'après de nombreux économistes et chercheurs, pour qu'une révolution industrielle ait lieu, il faudrait une nouvelle source d'énergie – de la même manière que nous avons connu successivement la vapeur, l'électricité, le pétrole. Or la révolution informatique des années 1970 ne possède pas une énergie propre, et pourtant, il s'agit bien d'une révolution.

Tentons d'adopter un raisonnement extrêmement simple : et si l'énergie de cette nouvelle révolution était tout simplement l'informatique, Internet ? En effet, l'économie et la société ne sont-elles pas au cœur d'une transformation radicale grâce (ou à cause) de cette révolution technologique ? La technologie blockchain, ou plus largement celle des grands livres distribués, n'est-elle pas portée, véhiculée et amplifiée par le réseau web ?

En ce cas, si nous admettons ce raisonnement, alors nous sommes en pleine révolution.

Don Tapscott, auteur de *Blockchain Revolution*[1], déclarait récemment : « Internet entre dans une deuxième ère. Nous avons eu l'Internet de l'information. Avec la blockchain nous voyons la montée de l'Internet de la valeur. Il existe de profondes possibilités d'améliorer l'économie et la gestion des États. »

L'analyse de maître Hubert de Vauplane[2]

« Si son utilisation devait être confirmée, la blockchain pourrait révolutionner le fonctionnement de nombreuses activités, à commencer par celles de la finance et des marchés financiers :

1. http://dontapscott.com/books/blockchain-revolution/. C'est le 3e ouvrage significatif de Don Tapscott après *Digital Economy* en 1994 sur le travail et la production collaborative *via* les technologies récentes de communication comme Internet, et *Wikinomics : How Mass Collaboration Changes Everything* en 2006 où il traite de l'intelligence collaborative.
2. Citation de Hubert de Vauplane, avocat, extraite d'un article publié dans Finyear.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

construits dès l'origine comme des organisations pyramidales et centralisées, les acteurs traditionnels se verraient alors en compétition avec de nouveaux entrants utilisant une architecture ouverte et décentralisée, plus propice à la mise en place d'une organisation horizontale tournée autour du client. »

Poursuivant ce parallèle avec le Web, de nombreux experts affirment que la blockchain semble aussi révolutionnaire que l'invention d'Internet. Dans les années 1990 et 2000, Internet a révolutionné la société parce qu'il a modifié la recherche de données ainsi que l'utilisation commune d'informations dans les communautés en ligne. « La blockchain va encore plus loin, explique Daniel Diemers, associé PwC Strategy& Suisse[1]. La blockchain permet la distribution et la gestion de pratiquement tous les types de données, dont les certificats de propriété, les valeurs réelles et numériques et même les données liées à l'identité. Bref, cette technologie offre la possibilité de distribuer, d'actualiser et de coordonner des listes électroniques pratiquement en temps réel. »

Nous serions en pleine destruction créatrice, synonyme de créations d'emplois et de marchés au détriment de la destruction d'autres emplois et marchés. Ainsi, en 1942, dans *Capitalisme, socialisme et démocratie*, Schumpeter explique que « le nouveau ne sort pas de l'ancien, mais apparaît à côté de l'ancien, lui fait concurrence jusqu'à le ruiner ».

Nous pensons que cette ère « Web 2.0 » avec Internet puis avec l'économie collaborative arrive à son point culminant avec la technologie blockchain car c'est elle qui va permettre, en s'appuyant sur le réseau Internet, l'Internet des objets et l'intelligence artificielle, de rendre plus intelligents l'énergie elle-même, les villes, les bâtiments, les automobiles, les industries, les

1. Extrait du rapport téléchargeable en fin d'ouvrage : « Blockchain : 5 propositions pour transformer les services financiers ».

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

échanges, etc. afin d'apporter à notre économie et notre société plus de transparence, de partage et de confiance.

Il semblerait donc que la technologie blockchain soit *la* prochaine révolution et que 2017 soit l'année où les organisations et, dans une moindre mesure, le grand public découvrent ses premières applications concrètes.

Pensées et visions

C'est la crise de confiance et de défiance des sociétés qui, au tournant de la crise de 2007-2008, a donné naissance à Bitcoin et ensuite à la technologie blockchain telle que nous la connaissons aujourd'hui. C'est à partir de ce moment qu'un esprit libertarien[1] a soufflé sur le monde de la finance et c'est aussi pour cela que les banques et d'autres institutions ont été les premières à réagir face à la progression du bitcoin et à tenter de s'approprier une technologie qui menaçait de les disrupter – technologie qui, par nature, est décentralisée et partagée par ses membres, et qui apporte confiance, partage et transparence. C'est cela la promesse de la blockchain.

Il serait illusoire de penser que l'économie et la société vont changer et se transformer en quelques mois à cause ou grâce à la technologie blockchain. En revanche, nous savons que le mouvement est désormais enclenché et que peu de choses pourront l'arrêter. Des initiatives sont lancées un peu partout dans le monde autour des crypto-monnaies et des blockchains publiques, des organisations publiques ou privées lancent de vastes projets blockchain internationaux, mais quid de cette

1. Le libertarianisme ou libertarisme est une philosophie politique issue du libéralisme qui prône, au sein d'un système de propriété et de marché universel, la liberté individuelle en tant que droit naturel.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

révolution annoncée ? Allons-nous vers un nouveau monde ? Notre mode de vie sera-t-il impacté ?

Voici trois pensées qui devraient nourrir notre réflexion.

L'économiste américain qui voulait remplacer le cash par le bitcoin

Kenneth S. Rogoff[1], ancien économiste en chef du Fonds monétaire international et professeur à Harvard, explique le but de la monnaie fiduciaire et son impact négatif sur l'économie.

Dans son récent ouvrage *The Curse of Cash*[2], et lors d'un déjeuner de presse début septembre 2016, Kenneth S. Rogoff a établi deux principaux facteurs à l'origine de sa motivation pour mettre un terme au cash : sa forte présence dans l'économie souterraine et l'incapacité du gouvernement américain à contrôler la circulation des espèces.

De l'argent comptant sur les marchés souterrains

Les instruments monétaires dits « anonymes » comme le bitcoin (sécurisé compte tenu de l'existence d'un registre public des transactions traçables) ont été largement considérés comme la principale monnaie de fonctionnement des marchés souterrains.

Une part importante du commerce illicite et des activités criminelles serait effectuée en utilisant des devises numériques, or il s'avère que la majorité de ces activités sont traitées avec de l'argent liquide en raison de son anonymat complet. Ainsi il devient pratiquement impossible pour les organismes

1. Économiste américain : http://scholar.harvard.edu/rogoff
2. http://press.princeton.edu/titles/10798.html

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

gouvernementaux de suivre le flux de trésorerie dans les transactions criminelles.

Voici pourquoi Kenneth S. Rogoff suggère que les gouvernements, en particulier le gouvernement fédéral des États-Unis, mettent un terme à l'argent liquide afin de réduire la circulation de l'argent et ainsi mettre fin à la plupart des opérations souterraines.

Taux d'intérêt négatifs

Kenneth S. Rogoff estime également que la mise en œuvre simultanée des taux d'intérêt négatifs par les banques centrales de premier plan dans le monde, y compris la Réserve fédérale, devrait aider à stimuler la croissance économique, car en théorie, un nombre croissant d'épargnants sortirait leur argent placé pour le faire circuler.

Certaines des plus grandes banques centrales et les banques commerciales ont déjà commencé à appliquer des taux d'intérêt négatifs. En réponse, les épargnants commencent à retirer leur argent des banques et à le stocker dans des endroits physiques, tels que des placards ou des micro-ondes, voire à le placer dans des achats de métaux précieux (or, argent, etc.) et donc à thésauriser à nouveau.

Le rôle du bitcoin

À partir du moment où les gouvernements commenceront à envisager d'abolir l'argent liquide, un système numérique ou un registre pour le règlement des devises et des actifs sera construit. À la pointe de la recherche et dans la droite ligne de ce raisonnement, certaines banques centrales comme la Banque d'Angleterre songent à utiliser la technologie blockchain pour construire des systèmes de devises numériques centralisés.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Dans le cas où ces réseaux de blockchains privées viendraient à émerger, les monnaies numériques dominantes comme le bitcoin seraient en forte demande, ce qui en augmenterait la valeur, ainsi que la présence et l'importance dans les plus grandes économies du monde.

Blockchain, révolution sociétale et économique[1] ?

Les valeurs promues par Internet dévoyées au profit d'un petit nombre

La révolution Internet de la fin des années 1990 était synonyme, à l'époque, d'un vent de liberté que beaucoup pensaient possible grâce à son ouverture, sa dimension internationale, hors de contrôle et sans règles. Et puis, en l'espace de quelques années, l'écosystème s'est organisé autour de grands pôles d'attractivité, de confiance, presque de nouveaux États, ceux qu'on appelle aujourd'hui les GAFA (Google, Amazon, Facebook, Apple) ou même encore plus récemment les NATU (Netflix, Airbnb, Tesla, Uber). Ce qui semblait permettre d'amener plus de pouvoir au peuple, hors de la mainmise des États sur l'économie réelle, a fini par se concentrer entre les mains de quelques individus à l'échelle du globe qui ont su mieux que les autres exploiter le système, se l'approprier et en extraire la valeur au détriment des autres. Un modèle qui aura mis vingt ans à se construire, à se structurer et à émerger pour ne laisser place qu'à quelques « happy few ». Alors effectivement, ces entreprises se sont créées et développées grâce à la liberté et la facilité d'entreprendre qu'a permis le Net, mais pour finir par concentrer toute la valeur hors du contrôle des États et surtout dans les poches de ceux qui ont su le mieux profiter du système.

1. Par Sébastien Bourguignon (voir remerciements en fin d'ouvrage).

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

La blockchain ou le retour de la confiance

Depuis quelques mois maintenant, on parle à tous les étages de la société, civile, économique, digitale et politique, d'une nouvelle révolution, une révolution numérique, celle de la blockchain. Cette technologie à la base de la crypto-monnaie bitcoin est qualifiée de « machine à créer de la confiance » par *The Economist*[1]. Elle serait la réponse à la crise de confiance générée par les systèmes politiques et financiers depuis de nombreuses années. Comment le ferait-elle ? Grâce à trois mécanismes constitutifs du système blockchain : la cryptographie asymétrique, les systèmes distribués et un modèle de fonctionnement pair à pair capable de générer du consensus de manière distribuée et sans tiers de confiance[2]. La blockchain serait donc devenue en peu de temps le nouvel espoir d'une disruption annoncée de tous les systèmes économiques, financiers et sociaux à base d'intermédiaires, autant dire que cela impacte une bonne partie des institutions, des États et plus globalement de tous les tiers spécialisés. On parle de la technologie qui serait capable d'ubériser Uber, un comble !

La blockchain porte donc les germes d'une révolution, celle-là même que l'on imaginait possible avec l'avènement d'Internet mais qui finalement n'a abouti qu'à plus de contrôle, d'opacité et d'hégémonie plus que de libertés individuelles et de partage de la valeur. Elle peut disrupter grâce à sa capacité à mettre en réseau des individus qui ne se connaissent pas, n'ont pas forcément confiance les uns envers les autres, pour les faire collaborer ensemble, leur faire créer de la valeur par leurs activités respectives et se la partager de manière équitable, transparente,

1. http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine
2. http://www.fondapol.org/wp-content/uploads/2016/06/083-SOUDOPLATOF-2016-05-26-webDEF.pdf

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

sécurisée et infalsifiable. Bitcoin, première implémentation de la blockchain, est d'ailleurs la preuve de ce nouveau modèle. En effet, en permettant à des personnes aux extrémités du globe de s'échanger de l'argent sans intermédiaire bancaire, de manière totalement décentralisée, transparente et sécurisée, en limitant au strict minimum les frais associés à cette transaction, la blockchain démontre son potentiel économique et social.

Une technologie démocratique

Elle est aussi fondamentalement démocratique. En tant que technologie, elle est basée sur le modèle *open source*, modèle qui a fait ses preuves depuis de nombreuses années dans le développement logiciel et qui aujourd'hui garantit une totale lisibilité du fonctionnement de la blockchain, en tout cas pour les initiés. Son développement initial et ses évolutions futures sont soumis à la volonté du peuple, les développeurs et utilisateurs, qui peuvent décider à tout moment d'accepter ce qui leur est proposé par la communauté ou le rejeter, ici encore le consensus est au cœur de l'évolution du système, au-delà d'être au cœur de la validation des transactions financières qui circulent en son sein. Et c'est d'ailleurs toute la vertu et toute la difficulté que représente ce modèle démocratique ; en effet, la gouvernance étant totalement décentralisée, sans consensus, il n'y a pas d'évolution possible des règles en place. Le système est donc totalement politique, tout est forcément soumis au vote, les luttes d'influence sont nécessairement présentes et la base des discussions étant technologique, seules deux options sont possibles : a) le vote en conscience parce qu'on dispose des compétences pour comprendre de quoi il retourne ; b) le vote aveugle basé sur la confiance accordée aux développeurs et utilisateurs les plus à même d'influencer.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Le risque de dérive vers une nouvelle forme de centralisation

On se rend bien compte que la décentralisation peut rapidement retomber sur une nouvelle forme de centralisation. Ainsi, on vient de le voir par la concentration du pouvoir de fonctionnement au travers des compétences techniques, mais ce point est vrai aussi pour ce qui est de la création de valeur au travers de la puissance de calcul allouée. Ainsi le minage, qui est la clé de voûte du processus de la blockchain, repose initialement sur un ensemble d'utilisateurs du réseau qui portent une partie de la responsabilité de la validation des transactions qui circulent et de leur inscription dans des blocs puis dans la chaîne de blocs. La difficulté grandissante de miner sur la blockchain Bitcoin – et c'est aussi le cas sur la blockchain Ethereum qui devrait d'ailleurs changer en 2017 de mode de consensus –, a forcé les mineurs à se regrouper en *pools* pour leur permettre d'augmenter leurs chances de miner des bitcoins et donc de créer de la valeur. Or, aujourd'hui, la puissance de calcul finit par se concentrer sur quelques dizaines de *pools* qui pourraient dans les années à venir posséder plus de 51 % de la puissance nécessaire pour permettre un acte de fraude tant redouté. Cette nouvelle forme de centralisation devra donc être traitée par les développeurs et les utilisateurs de la technologie pour éviter les dérives, mais là aussi cela ne pourra se faire sans le consensus de tous.

Une technologie en plein essor dont il faut encore poser des jalons

Il y a aussi de nouvelles formes d'organisations apportées par la technologie qui sont extrêmement prometteuses avec les DAO. Elles vont permettre d'aboutir à de nouvelles formes d'organisations sans pouvoir central et basées sur une gouvernance décentralisée. Les individus vont pouvoir se regrouper les uns avec les autres, être contributeurs à un ou plusieurs projets sans avoir de

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

liens hiérarchiques entre eux. En sous-jacent, cela implique un meilleur partage de la valeur entre les acteurs puisque celle-ci est gérée par le code. Mais en cas de désaccord ou de conflit, qui arbitrera ? En cas de défaillance de l'organisation ou de détournement de celle-ci, contre qui pourra-t-on se retourner ?

Il y a donc encore bien des défis à surmonter pour que la blockchain devienne la révolution numérique tant annoncée. Elle est pour le moment l'objet de toutes les attentions du petit monde des spécialistes du numérique. Si l'on s'en tient à la courbe de la « hype de Gartner », la chaîne de blocs est aujourd'hui dans la phase des « pics des espérances exagérées[1] ». Nous en sommes donc à la phase juste avant celle du « gouffre des désillusions », en général une période de traversée du désert pour une technologie. Cela ne veut pas dire que la blockchain risque de tomber dans les oubliettes, ni même que les start-up et projets qui se seront lancés sur cette technologie aujourd'hui ne réussiront pas, mais simplement qu'il y a avant tout besoin de se l'approprier pour pouvoir évaluer en conscience les opportunités sociétales et économiques qu'elle peut représenter.

La blockchain comme révolution… mais révolution de quoi[2] ?

Les questions que pose la blockchain sont extrêmement nombreuses[3]. Au-delà de celles largement débattues autour de

1. Un pic des espérances exagérées peut être défini comme « un emballement médiatique qui aboutit à des attentes exagérées et non réalistes. Des start-up se créent pour développer et commercialiser des produits basés sur la nouvelle technologie » (source : Wikipédia).
2. Par Alain Brégy (voir remerciements en fin d'ouvrage).
3. Lire ce texte intégral : https://medium.com/@beAchain/blockchain-comme-révolution-mais-révolution-de-quoi-8acc059bf316#.fb4ynqv44

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

son utilisation réelle ou potentielle (disruption des tiers de confiance, sécurisation des échanges, gages d'authentification, technologies de partage de ressources, économies d'échelles, garantie des transactions, auto-exécution de contrats, décentralisation des processus, etc.) un certain nombre d'autres plus complexes à explorer se pose.

L'histoire des sociétés n'est jamais lisse ni linéaire. À des périodes de bouleversements brutaux généralement très rapides – souvent en moins de deux ou trois générations – succèdent de grandes époques beaucoup plus longues, durant souvent plusieurs siècles, où les acquis de ces courtes périodes de bouleversements fondent un réel commun satisfaisant plus ou moins la société. S'ils sont sans cesse réaménagés, corrigés, repris, améliorés, modifiés, il n'en reste pas moins que ces acquis forment un socle stable à partir duquel la vie en société est possible.

Révolutions et changements radicaux

Le monde des sociétés occidentales modernes tel qu'on le connaît actuellement a, pour faire court, moins de deux siècles. Il date de la Révolution de 1789 et de la révolution industrielle qui a suivi au XIX^e^ siècle. Les grands bouleversements précédents ont été principalement la Renaissance vers le XIV^e^ siècle puis les Lumières entre le XVI^e^ et le XVII^e^ siècle.

Chacune de ces époques de changements radicaux – le monde tel qu'on le décrit et tel qu'on le vit n'est d'un coup plus du tout le même – a créé les outils dont elle avait besoin pour lui permettre d'accompagner et de réaliser ces changements ; on pense par exemple à l'imprimerie qui, originellement, avait été inventée en plein monde médiéval pour diffuser massivement la doctrine de la foi chrétienne et qui, au bout du compte, a surtout été utile à la modernité de la Renaissance pour diffuser ses thèses humanistes émancipatrices. On voit à travers cet exemple qu'une technologie quelle qu'elle soit peut donc être

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

à la fois incrémentale – elle sert à améliorer, à modifier, à transformer la société mais sans jamais remettre en cause ses fondements ni les façons qu'elle a de décrire la réalité qu'elle vit (comme l'a été par exemple le passage de la machine à vapeur à la machine électrique qui a transformé toute l'industrie sans remettre en question les fondements purement économiques du « comment produire ») – et disruptive.

La blockchain cristallise cinq valeurs

Ce qui distingue et qualifie une technologie est donc, au-delà de ce pour quoi on dit qu'elle est faite, ce qu'elle porte ou ne porte pas comme nouvelle façon de voir et de dire le monde.

Il est probable qu'à travers la blockchain, ce soit en définitive notre monde qui, engagé dans toute une série de mutations extrêmement profondes, si profondes qu'elles remettent en question tout notre modèle sociétal patiemment édifié depuis près de deux siècles, trouve à exprimer quelques-uns des grands enjeux qui le traversent.

La blockchain en cristallise au moins cinq : la valeur, la monnaie, le travail, l'être-individu et la question démocratique. Elle peut bien sûr être techniquement utilisée pour répondre à d'autres enjeux tout aussi importants (par exemple la préservation de l'environnement, la gestion de l'énergie, etc.) mais elle ne me semble pas les porter intrinsèquement en elle, dans sa construction même, alors que ces cinq-là sont directement questionnés par la blockchain.

En limitant ses potentialités aux champs connus et reconnus de l'économie (échanges monétaires décentralisés, transactions simplifiées, éviction d'intermédiaires coûteux), de la production (modélisation de l'entreprise 4.0 de demain, les DAO), de l'applicatif pur (sécurisation des échanges et des données) ou de la gouvernance (décentralisation, consensus), on s'empêche

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

toute vision prospective de la blockchain ; la restreindre à ces fonctions, c'est ne pas la prendre en compte dans sa perspective historique large.

Ici, nous abordons successivement les questions de la valeur (comment s'évalue-t-elle, à partir de quels présupposés initiaux), de la monnaie (à quoi sert-elle, que vaut-elle, qui l'émet), du travail (qu'est-ce que produire), de l'identité (comment nous définissons-nous) puis enfin de l'organisation politique des sociétés (selon quels modes de gouvernance), montrant comment la blockchain porte en elle des modèles théoriques potentiels qui dépassent de très loin ce pour quoi elle semble être faite.

L'émergence de la blockchain

Au-delà de ce qui se dit, des séries de « pratiques » apparaissent autour de la blockchain comme autant d'énoncés venant parfois infirmer ou contredire ce qui est dit. Exactement de la même façon que la question « qu'est-ce que le Web et à quoi sert-il ? » aura reçu des réponses radicalement différentes selon qu'on l'aura posée en 1996, en 2006 ou en 2016, la question « qu'est-ce que la blockchain et à quoi sert-elle ? » ne trouvera pas sa solution dans une collecte exhaustive recensant l'intégralité des formulations à son sujet, mais dans l'étude et l'observation de ses pratiques. Comment est-elle utilisée et pour en faire quoi nous en apprendra plus que toutes les prédictions/divinations émises çà et là.

C'est dans cet interstice entre « dire » et « faire » que la blockchain est actuellement en train d'émerger. Dire, c'est se placer le plus souvent dans le seul registre économique ; c'est en endosser à la fois la logique, le lexique et les outils conceptuels, en déclarant par exemple que « la blockchain nous fera réaliser d'importantes économies ». C'est vrai mais c'est faux.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

C'est vrai comme effet de bord immédiat à très court terme, mais c'est faux comme probable réorganisation de toute la production de richesses à plus long terme.

La blockchain n'est que l'outil d'un monde entré en révolution

La blockchain n'est pas une révolution. Elle n'est que l'outil d'un monde lui-même entré en révolution. Et donc, paradoxalement, dire aujourd'hui ce qu'est la blockchain revient le plus souvent à énoncer ce que le monde de demain ne sera probablement plus. Et parce que la blockchain n'est ni une technologie ni une révolution, elle ne peut ni être décrite sous l'angle de sa capacité à disrupter, ni être réduite à la technique qui la sous-tend sans prendre le risque de passer à côté de ce qui, au fond, est peut-être sa nature originelle : n'être qu'un artefact au service d'un changement de civilisation, changement qui s'annonce comme au moins aussi radical et aussi dévastateur qu'ont pu l'être en leurs temps la Renaissance, les Lumières ou les révolutions industrielles pour leurs propres « empires du passé ».

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Copyright © 2017 Eyrolles.

Conclusion

Lorsque Internet fit son apparition dans les années 1990, les experts prédisaient une révolution. Un grand bouleversement technologique, économique et sociétal nous attendait avec son cortège de pertes d'emplois et de transformations diverses et variées.

Trente années se sont écoulées depuis cette apparition et nous devons reconnaître que si la révolution n'a pas été ce Big Bang annoncé, les évolutions technologiques successives ont transformé un grand nombre de modèles d'affaires, ainsi que l'économie et la société elle-même, et ce, bien au-delà des limites et des usages que ses pères fondateurs avaient imaginés. En revanche, le Web n'a pas complètement réussi son pari de plus de confort, plus de liberté et plus de pouvoir pour l'humain.

De la « simple » architecture technique qu'était le Web à ses débuts, nous avons successivement connu un Web des contenus (blogs), puis un Web marchand (e-commerce), puis les générations X et Y[1] ont inventé le Web social (Facebook, Instagram, etc.) avec de nouveaux usages et en y ajoutant en particulier plus de partage, de transparence, ce qui a entraîné une totale transformation sociétale et économique. Ce Web social a amplifié la mutualisation des contenus, le commerce instantané et collaboratif, la prise de parole citoyenne et les réseaux collaboratifs.

Mais le Web n'a pas stoppé son évolution, il l'a poursuivie avec de nouveaux usages et des modèles prometteurs comme

1. La génération X regroupe les personnes nées entre 1966 et 1976 (environ), la génération Y, celles nées entre le début des années 1980 et le milieu des années 1990.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

BlaBlaCar, Airbnb et Uber et au passage, il a inventé l'ubérisation – qui consiste à créer des plateformes de désintermédiation.

Au fil des années, les entreprises se sont en grande partie approprié cette offre internet et aujourd'hui, elles découvrent une nouvelle technologie, la blockchain, mais également les promesses qu'elle contient – car ce n'est pas le caractère destructeur de la blockchain qu'il faut retenir mais son caractère disruptif qui peut transformer et améliorer la grande majorité des modèles d'affaires.

Demain, le grand public va découvrir, à travers la technologie des blockchains et des protocoles de consensus distribués, la désintermédiation, les monnaies numériques, les transactions instantanées à des coûts proches de zéro, voire gratuites, les places de marché et les réseaux sociaux sans intermédiaire (tiers de confiance), les assurances collectives sans organe central de contrôle, les voitures autonomes et partagées, la démocratie transparente, l'énergie et les villes intelligentes, etc.

Depuis la crise financière de 2008, nous avons perdu confiance en nos banques et nos institutions financières, puis progressivement en nos personnels politiques, nos administrations, l'État… Aujourd'hui, nous offrons notre confiance à notre communauté, à l'« autre nous », à celui qui nous correspond, qui nous ressemble, notre alter ego, et nous cherchons des nouvelles forme de gouvernance.

C'est un monde nouveau qui se profile. Après être successivement passés par un monde de transparence avec des médias décentralisés, autonomes et instantanés, puis par un monde de partage avec les réseaux sociaux et les espaces collaboratifs (wiki) qui ont progressivement envahi toute la société en grande partie grâce aux réseaux et aux terminaux mobiles, nous voyons aujourd'hui poindre la confiance (*trust*) partagée et de nouveaux usages grâce à la technologie blockchain.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Ce que le Web a initié et développé, la technologie blockchain va maintenant l'amplifier. Elle va engager de profondes mutations grâce à la désintermédiation et les protocoles de consensus. C'est tout un monde qui sera désintermédié, Uber lui-même sera désintermédié et ce sera l'ubérisation ultime prédite par Philippe Herlin[1].

La blockchain réussira peut-être ce pari initié par le Web de placer plus d'humain, de liberté et de confiance au cœur de sa technologie et ainsi nous faire passer progressivement d'un monde *wikinomics* (collaboratif) à un monde *trustnomics*[2] (confiance)… c'est tout cela que nous devons construire.

Nous voici arrivé au terme de notre voyage parmi les solutions blockchain et nous demeurons très optimistes quant à leurs possibilités, leurs multiples applications et leur potentielle disruption dans de très nombreux domaines d'activité ainsi que dans l'économie et dans la société.

Mais la blockchain n'est pas la révolution tant annoncée, « elle n'est que l'outil d'un monde lui-même entré en révolution[3] ».

1. Philippe Herlin, économiste et auteur de *La Révolution du bitcoin et des monnaies complémentaires*.
2. http://www.trustnomics.net
3. Citation d'Alain Brégy (voir remerciements en fin d'ouvrage).

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Copyright © 2017 Eyrolles.

Remerciements

Parce qu'un livre est le fruit d'une collaboration et non d'une écriture solitaire (*a fortiori* sur le sujet d'une technologie collaborative !), je voudrais remercier et exprimer ma gratitude à chacun des experts qui ont su me guider, me conseiller et m'éclairer de leur savoir tout au long de ce parcours et qui ont contribué à faire que ce livre existe.

Agosti Pascal

Pascal Agosti est avocat associé au cabinet Caprioli & Associés (Barreau de Nice). www.caprioli-avocats.com

Spécialiste en droit des nouvelles technologies, de l'informatique et de la communication.

Réussite à l'examen de Lead Auditor ISO 27.001.

Docteur en droit.

Titulaire d'un DEA de droit des contrats d'Affaires.

- Responsable du pôle « Contrats informatiques et électroniques » et du pôle « dématérialisation » ;
- Chargé d'enseignement à l'université de Nice Sophia-Antipolis, Master II « Droit des TIC » et à l'université de La Rochelle, Master II « Tiers de Confiance ».

Bourguignon Sébastien

Sébastien Bourguignon est manager au sein d'OCTO Technology, cabinet de conseil en IT et il est expert de la blockchain. Il est passionné par le numérique, l'innovation et les start-up. Il a créé un blog pour y partager l'actualité autour de ces thématiques et il a développé le projet #PortraitDeStartuper dans lequel il fait intervenir des start-upers qui présentent leur

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

retour d'expérience dans leur aventure entrepreneuriale. Par ailleurs, il publie régulièrement de nombreux articles sur des plateformes comme Le Cercle Les Échos, Siècle Digital ou encore Le Journal du Net. http://sebastienbourguignon.com et http://www.octo.com

Brégy Alain

Activiste de l'e-démocratie/e-citoyenneté, des communs et des monnaies libres, Alain Brégy est le fondateur de Vol de nuit, une entreprise dédiée aux usages numériques innovants : intelligence artificielle, réalité augmentée, applicatifs réseaux, plateformes de partage, solutions blockchain. Il est également cofondateur de l'association de France Blocktech, association de l'écosystème blockchain français et initiateur du groupe Blockchain Alsace. http://e-vdn.com/ (Vol de nuit) et http://www.france-blocktech.org

Chriqui Vidal

Vidal Chriqui est un expert en big data et systèmes distribués, ce qui l'a conduit très tôt à s'intéresser à la technologie du Bitcoin et aux différentes variantes de blockchain. Il a animé la première vidéo-série francophone *Blockchain Révolution* sur le bitcoin et la blockchain. Dans une vision blockchain des objets, Vidal se focalise sur les protocoles de registres distribués ouverts dans l'univers des objets connectés ainsi qu'aux protocoles de microtransactions (*micropayment channel*). http://www.sii.fr

Comparini Luca

Luca Comparini est responsable blockchain pour IBM France depuis septembre 2015. Avec plus de dix ans d'expérience sur les infrastructures IT, il se définit comme un *business-oriented geek* passionné de l'écosystème *open source* et des domaines

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

d'innovation, comme les technologies blockchain, les objets connectés et l'informatique cognitive. https://www.linkedin.com/in/lucacomparini

Croizeaux Fabrice

Fabrice Croizeaux est diplômé de Centrale Lyon et de HEC. Il est directeur général de InTech, une société luxembourgeoise de 100 personnes spécialisée dans le conseil en systèmes d'information et en développement d'applications spécifiques. InTech accompagne ses clients dans l'utilisation de technologies émergentes pour créer des innovations de rupture. Passionné de culture numérique, de développement et d'architecture, Fabrice est convaincu que l'utilisation des principes de confiance décentralisée sur lesquels reposent les blockchains peut révolutionner de nombreuses activités dans l'ensemble des secteurs. http://www.intech.lu

De Vauplane Hubert

Hubert deVauplane est avocat, *partner* à Kramer Levin (Financial and Banking law, Alternative Financing, Asset Management, Digital Payment) et administrateur de France Blocktech, association de l'écosystème blockchain français. http://www.kramerlevin.com/attorneys/detail.aspx?attorney=8541b423-94a6-4807-87d0-809ca2362231&l=French (biographie) et http://www.france-blocktech.org

Delahaye Jean-Paul

Jean-Paul Delahaye est informaticien et mathématicien, professeur à l'université de Lille 1. Il a publié de nombreux articles en ligne. https://bitcoin.fr/?s=delahaye et http://www.scilogs.fr/complexites/ (blog).

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Henocque Laurent

Laurent Henocque est polytechnicien, docteur en informatique habilité à diriger les recherches. Enseignant-chercheur dans les domaines de l'intelligence artificielle, du génie logiciel et des interfaces homme-machine. Des travaux sur le Web sémantique l'ont conduit à imaginer, puis à créer KeeeX. Cette société exploite plusieurs brevets relatifs à une technologie révolutionnaire de protection et chaînage des fichiers autoportés. http://www.KeeeX.me/fr

Mougayar William (auteur de la préface de ce livre)

William Mougayar, basé à Toronto, est investisseur, chercheur, blogueur et auteur de *The Business Blockchain* (Wiley, 2016). Il est un participant actif sur le marché de la crypto-technologie et conseiller ou membre du conseil d'administration de certaines des plus importantes sociétés mondiales de technologie blockchain, dont Ethereum, OpenBazaar, Coin Center et Bloq. Il rédige régulièrement des articles sur le présent et l'avenir des blockchains dans *Startup Management*. http://startupmanagement.org/blog/

Noizat Pierre

Pierre Noizat est blogueur[1] (e-ducat), secrétaire général de l'association Bitcoin-France.org et cofondateur de Paymium.com. Il est l'auteur de *Bitcoin, mode d'emploi*, paru en janvier 2015 sur Amazon et Lulu.com, en version papier (130 pages) et e-book (Kindle, etc.). http://e-ducat.fr/

1. « Je publie ce blog pour faire connaître les avantages de la diversité monétaire et questionner l'idée qu'un monopole local de l'euro serait souhaitable ou nécessaire. L'argent-dette, imposé comme monnaie unique, favorise la capture réglementaire par une oligarchie et l'accroissement des inégalités… »

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Péchoux Arnaud

Arnaud Péchoux est manager au sein du « Practice Financial Service » de Wavestone. Il pilote des grands projets de transformation dans le domaine de la banque, des assurances et de l'industrie du retail. Il anime également le lab blockchain de Wavestone qui a pour objectif d'accompagner ses clients dans la découverte et l'exploitation des potentiels du protocole blockchain. https://www.wavestone.com/fr/

Rouphael Romain

Romain Rouphael est CEO de la start-up Belem. http://www.belem.io/

Schmitt Jean-Luc

Jean-Luc Schmitt est cofondateur et animateur du site Bitcoin.fr. https://bitcoin.fr

Teruzzi David

David Teruzzi est rédacteur du blog blogchaincafe.com, spécialisé dans la blockchain et son univers, expert pour les quotidiens en ligne Finyear.com et BlockchainDailyNews.com, consultant blockchain, directeur technique et cofondateur de blockchain-conseil.fr, développeur affilié du projet decred.org et programmeur expert en mathématiques appliquées. http://www.blockchain-conseil.fr

Verbiest Thibault

Thibault Verbiest est avocat associé du cabinet De Gaulle Fleurance & Associés. Il dispose d'une expérience approfondie notamment en propriété intellectuelle et dans le secteur des technologies, des médias et des télécommunications.

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Formation : inscrit aux barreaux de Bruxelles et de Paris depuis 1993. Titulaire d'un master en *international entertainment law* (University of San Diego), d'un master de droit économique et en droit public (université libre de Bruxelles). http://www.degaullefleurance.com/equipe/thibault-verbiest-2/

Vergne Nicolas

Nicolas Vergne est étudiant ESSEC passionné par le monde de la blockchain. Nicolas a écrit un petit essai, *Tour d'horizon de la blockchain*. Contact : hello[at]finyear.com

Je remercie également **Pierre Leloup**, mon fils, graphiste des médias Finyear et Blockchain Daily News et illustrateur de ce livre. http://www.leloup.graphics/

Et un grand merci à vous, lecteur, d'avoir passé un peu de votre temps à parcourir ce petit livre, qui, je l'espère, aura, au moins partiellement, répondu à vos questions, alimenté votre réflexion et aidé à la mise en pratique de votre projet autour de ces technologies naissantes et novatrices que sont les blockchains et les protocoles de consensus distribués.

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Ressources

Glossaire

Retrouvez l'ensemble des définitions de cet ouvrage sur http://www.blockchaindailynews.com/glossary/

Rapports – Études

Blockchain, ressources, rapports, études (2000-2016) sur http://www.blockchaindailynews.com/Blockchain-ressources-rapports-etudes-Resources-reports-studies-2000-2016_a24877.html

Médias français

Bitcoin.fr : https://bitcoin.fr

Bitconseil.fr : http://www.bitconseil.fr

Blockchain Daily News : http://www.BlockchainDailyNews.com

Blockchain France : https://blockchainfrance.net/

Blogchain Café : http://blogchaincafe.com/

E-Ducat : http://e-ducat.fr/

Finyear : http://www.finyear.com

La Voie du Bitcoin : http://blog.lavoiedubitcoin.info/

Le Coin Coin : https://le-coin-coin.fr/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Forums

http://www.bitcointalk.org : section française du tout premier forum consacré à Bitcoin, initié par Satoshi Nakamoto

cryptofr.com : forum en français dédié aux monnaies décentralisées

Quora – Cryptocurrencies : https://www.quora.com/topic/Cryptocurrencies

Podcasts – Vidéos – Cours

https://epicenterbitcoin.com/

http://thebitcoinpodcast.com

http://nipcast.com/category/nipcoin

https://www.udemy.com/ : cours en anglais (vidéos)

https://www.khanacademy.org/ : cours en anglais (vidéos)

https://www.coursera.org/ : cours en anglais (textes)

https://openclassrooms.com/ : cours en français (textes)

http://www.blockness.io : formation techno blockchain

Associations

Bitcoin France : https://bitcoin-france.org/

Blockchain Valley (incubateur-académie) : http://www.blockchain-valley.fr

France Blocktech : http://www.france-blocktech.org

La Chaintech : https://www.chaintech.fr/

Le Cercle du Coin : http://lecercleducoin.fr/

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Ouvrages

2008

Nassim Nicholas Taleb, *Le Cygne noir, la puissance de l'imprévisible*, Les Belles Lettres

2012

Pierre Noizat, *Bitcoin, monnaie libre*, e-book

Pierre Noizat, *Bitcoin Book*, e-book

Daniel Kahneman, *Système 1/Système 2, les deux vitesses de la pensée*, Flammarion

2013

Philippe Herlin, *La Révolution du bitcoin et des monnaies complémentaires*, Eyrolles

Serge Roukine, *Comprendre et utiliser le Bitcoin*, 19éditions

Nassim Nicholas Taleb, *Antifragile, les bienfaits du désordre*, Les Belles Lettres

2015

Andreas Antonopoulos, *Mastering Bitcoin*, O'Reilly (traduction française PDF : http://e-ducat.fr/download/mastering_bitcoin.pdf)

Pierre Noizat, *Bitcoin, mode d'emploi – L'invention d'une liberté*, e-book

Jeffrey Tucker, *Bit by Bit – How P2P Is Freeing the World*, Liberty.me

Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller et Steven Goldfeder, *Bitcoin and Cryptocurrency Technologies*, Princeton University Press

Melanie Swan, *Blockchain*, O'Reilly

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

2016

Blockchain France, *La Blockchain décryptée – Les clefs d'une révolution*, Netexplo

Andreas Antonopoulos, *The Internet of Money*, e-book

Alex et Don Tapscott, *Blockchain Revolution : How the Technology Behind Bitcoin Is Changing Money, Business, and the World (2016)*, Porfolio

Paul Vigna et Michael J. Casey, *The Age of Cryptocurrency : How Bitcoin and the Blockchain Are Challenging the Global Economic*, Picador

Roger Wattenhofer, *The Science of the Blockchain*, e-book

Didier Geiben, Olivier Jean-Marie, Thibault Verbiest et Jean-François Vilotte, *Bitcoin et Blockchain : Vers un nouveau paradigme de la confiance numérique ?*, La Revue Banque

William Mougayar, *The Business Blockchain : Promise, Practice, and Application of the Next Internet Technology*, Wiley

Henning Diedrich, *Ethereum : Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*, Wildfire Publishing

Arvind Narayanan et Joseph Bonneau, *Bitcoin and Cryptocurrency Technologies : A Comprehensive Introduction*, Princetown University Press

Nathaniel Popper, *Digital Gold : The Untold Story of Bitcoin*, Harper

Éric Alton, *Blockchain : The Beginner's Guide to the Economy-Revolutionizing Technology*, e-book

Terry Parker, *Smart Contracts : The Ultimate Guide To Blockchain Smart Contracts – Learn How To Use Smart Contracts For Cryptocurrency Exchange*, e-book

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Ghassan Karame et Elli Androulaki, *Bitcoin and Blockchain Security*, Artech House Publishers

Timothy Short, *Blockchain : The Comprehensive Guide to Mastering the Hidden Economy*, e-book

Acteurs

Plateformes de change – Où acheter des bitcoins et/ou d'autres crypto-monnaies

Seules les 20 premières (suivant les notes des utilisateurs) sont référencées[1] :

anxbtc.com / anycoindirect.eu / belgacoin.com / bitboat.net (FR) / bitcoin.de / bitcurex.com / bitit.gift (FR) / bitstamp.net / bity.com (CH) / btc-e.com / coinbase.com / coinhouse.io (FR) / flipco.in (FR) / kraken.com / lamaisondubitcoin.fr (FR) / localbitcoins.com / mineoncloud.com (FR) / paymium.com (FR) / safello.com / virwox.com

Citons un cas à part : Uphold.com (anciennement BitReserve), plateforme garantissant contre la volatilité du bitcoin.

Explorateurs de blockchains et agrégateurs de données Bitcoin

bitcoinchain.com / bitcoinfees.21.co : calcul des frais de transaction / biteasy.com / bitnodes.21.co : données / blockchain.info (FR) / btc.blockr.io / chainflyer.bitflyer.jp / coinplorer.com / coinprism.info / goochain.net / kaiko.com (FR) / oxt.me (FR) / thehalvening.com (FR) /

1. Classement réactualisé chaque mois sur : https://bitcoin.fr/acheter-bitcoin/

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Matériel de minage (Bitcoin / Altcoins)

mineoncloud.com : mineurs Asic SHA-256, mineurs Asic Scrypt, contrats de minage

la-boutique-du-mineur.com : matériel de minage (Bitcoin et autres altcoins)

rigs.ch : matériel de minage (châssis en aluminium, risers et autres accessoires)

antminerdistribution.com : distributeur européen de mineur de la marque Antminer

Sécurité

badbitcoin.org : liste noire des escroqueries liées à Bitcoin et aux monnaies décentralisées.

bittrust.org : évaluation des commerces et des services en relation avec Bitcoin

blockchainalliance.org : association de lutte contre la cybercriminalité sur la blockchain

blockchaininspector.com : surveillance de la blockchain, identification et localisation des activités criminelles

chainalysis.com : surveillance de la blockchain, identification et localisation des activités criminelles

sabr.io : surveillance de la blockchain, identification et localisation des activités criminelles

scorechain.com : analyse et évaluation des adresses Bitcoin

Compagnies Blockchain, Bitcoin, Ethereum, etc.

Plutôt que dresser une liste de plus de 300 noms et liens, nous vous proposons de visiter le « Top des compagnies &

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

startups blockchain » mis à jour régulièrement sur le quotidien Blockchain Daily News :

http://www.blockchaindailynews.com/Top-250-blockchain-companies-startups_a24712.html

Copyright © 2017 Eyrolles.

© Groupe Eyrolles

Copyright © 2017 Eyrolles.

Index

A

Accenture 90
achat de bitcoin 37
ACINQ 69
adresse bitcoin 19, 51
algorithme de consensus personnalisable 110
altcoins 56
alternative cryptocurrencies 56
anonymat 50, 109
arbre de Merkle 30
argent liquide 190
ArtTracktive 128
Ascribe 72
attaque à 51 % 49
auditabilité 110
augmentation de la taille des blocs 63
authentification 128
autorité centrale 34

B

Back Adam 65
beAchain 103, 113, 114
Belem 150, 152
BigchainDB 71
bitcoin 20, 21, 33, 190
Bitcoin 18, 33, 153
BitcoinCore 42
bitgold 29
BitGold 31, 79
BitShares 60
Blackcoin 60
blockchain databases 70
blockchain de consortium 94, 161
Blockchain Delaware Initiative 129
blockchain des données 153
blockchain hybride 94
blockchain privée 91, 94, 166
blockchain publique 76, 91, 93, 167, 188
Blockness 128
blocktech 159
b-money 29
Buterin Vitalik 73, 117

C

cadastre 140
cas d'usage blockchain 163
centralisation 122, 194
chaîne de blocs 13
chaînes collatérales 64
chiffrement à double clé 38
clé privée 18
clé publique 18
Codius 82
Colored Coins 62
confiance 192

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

confidentialité 110
Conscoin 60
conseiller en investissements participatifs 144
consensus 41, 97
consensus distribué 123
consommation énergétique 43
contrefaçon 138
Corda 112
Counterparty 63
crypto-devise 20, 42
cryptographie 13, 17, 94, 154, 167
cryptographie asymétrique 18, 29, 38, 192
crypto-monnaie 20, 42, 57, 106, 188

D

DAO 78, 83, 194
Dapp 105
Dash 60
décentralisation 122, 146, 193
decentralized autonomous organization 78, 83
délégation de preuve de possession 100
Deloitte Luxembourg 128
démocratie 193
désintermédiation 124
DigiCash 30
disruption 22, 121, 160
distributed ledger 91, 123
documents administratifs 140
données médicales 139
double dépense 34

E

éducation 155
e-Krona 57
énergie 134
essais cliniques 126
ETH 77
ether 74
Ethereum 73, 85, 153, 194
éthique 60

F

fichier bancaire FIBEN 145
fiducie 87
financement participatif 144
Fintech 159
Flare 70
force juridique 170, 172
forum Bitcointalk 33

G

gaz 78
Gnutella 31
Goldman Sachs 23
gouvernance 170, 193
gouvernance 2.0 83
grand livre distribué 91, 123

H

hacker 88
HashCash 31, 65

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

Herlin Philippe 21
historique blockchain 51
horodatage 34, 151
Hyperledger 22, 26, 108

I

IBM France 25
identité numérique 141
immutabilité 126
inaltérabilité 146
infalsifiabilité 80, 126, 193
Interledger 110, 111
Internet 16
Internet des objets 107, 157
IOTA 107, 158
irréfutabilité 80
irrévocabilité 126

K

KeeeX 154
key-image 54
Know-Your-Customer (KYC) 52, 59
Kuovola Innovation 153

L

langage Turing-complet 76, 81
Lightning Network 67
Lisk 103
livre de compte 13, 34
logiciel libre 171
lutte contre le piratage 137

M

masternodes 53
Mazacoin 59
mega-pools 48
micro-grid 135
minage 41, 98, 124
mineur 41, 48, 78, 165
Monax 112
Monero 53
monnaie fiat 54
monnaie numérique 20

N

Nakamoto Satoshi 32
nœud 41, 93
notarisation 128

O

OneCoin 59
Oracle 82
organisations virtuelles temporaires (QVO) 116

P

paiements électroniques 143
Paxos 47
Perez Carlota 179
performance 168
personnalité juridique 86
porte-monnaie 39
Potcoin 59
preuve datée digitale 80
preuve d'enjeu 98

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

preuve de travail 41
problème des généraux byzantins 44
proof of concept 147
proof of stake 52, 77, 99, 124
proof of work 41, 46, 52, 92, 95, 98, 99, 124, 167
propriété intellectuelle 151
protocole cryptographique 34
protocole libre 13
protocole SMTP 73, 122
pseudonyme cryptographique 51
puissance de calcul 13
puissance de calcul informatique 41

R

R3CEV 22, 112
registre 17
registre 2.0 14
registre distribué 163
registre distribué ouvert 92
règlement eIDAS 142
règlement livraison 143
réseau pair à pair 17, 34, 36
réversibilité 175
révolution industrielle 179
révolution informatique 182
RFID 153
Riksbank 57, 58
Ripple 106
Rogoff Kenneth S. 189
Rootstock 66

S

Santander Banco 22
scalabilité 109, 110
sécurité 125, 193
sidechains 56, 64
side databases 70
signature de cercle ponctuel 53
smart contract 31, 78, 79, 174
smart grids 135
Solidity 81
Stellar Consensus Protocol 105
supply chain 152
système distribué 29, 192
Szabo Nick 79

T

Tapscott Don 186
taux d'intérêt négatifs 190
technologie pair à pair 31
Tendermint 47, 111
The DAO 85, 88, 174
tiers de confiance 15, 20, 93, 121, 124, 164
token 92
tolérance aux pannes 47
traçabilité 127
traçabilité alimentaire 137
transaction bitcoin 32
transparence 126, 192

U

Uber 192
unités du bitcoin 40

Copyright © 2017 Eyrolles.
© Groupe Eyrolles

V

valeur du bitcoin 39
vérification décentralisée 80
Viacoin 60
Voatz 150
vote numérique distribué 148

W

wallet 39
Web 2.0 182

Z

Zcash 53, 60

© Groupe Eyrolles